NIST Special Publication 800-4

COMPUTER SECURITY CONSIDERATIONS IN FEDERAL PROCUREMENTS: A Guide for Procurment Initiators, Contracting Officers and Computer Security Officials

Barbara Guttman
March 1992

EXECUTIVE SUMMARY

The Computer Security Act of 1987 (Pub. L. 100-235) and Office of Management and Budget Circular A-130 mandate that U.S. Government agencies protect automated information and the resources used to process it (hardware, firmware, and software). OMB Circular A-130 specifically mandates that, as a part of protecting computer systems, agencies incorporate computer security in the system acquisition process. This NIST Special Publication provides guidance for federal procurement initiators, contracting officers, and computer security officials on including computer security in acquisitions.

To accomplish this goal, computer security and federal information processing (FIP) procurement must be integrated. Computer security is the protection of the integrity, availability and confidentiality of automated information and the resources used to enter, store, process, and communicate the information. Computer security shares properties with systems/software engineering including trustworthiness, system safety, and reliability. FIP procurement is the process of acquiring hardware, software, firmware, computer-related services and telecommunications. FIP procurement begins with the process of determining needs and ends with contract completion.

The integration of computer security and FIP procurement will result in improvements in:

- meeting agency missions;
- protecting federal assets; and
- protecting individual rights.

The integration is accomplished by incorporating computer security into all phases of the procurement cycle: planning, solicitation, source selection, and contract administration and closeout.

This guideline is based on the collective experience of government and industry personnel from the fields of computer security, procurement, and information resources management and is intended to be used in conjunction with agency or General Services Administration guidance on procurement and computer security. This guideline neither addresses nor supersedes requirements for the protection of national security information resources.

NIST has prepared a related document that addresses the area of computer security and procurement, Sample Statements of Work for Federal Computer Security Services, which provides assistance to agencies that are contracting for computer security services, such as performing a risk analysis.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
01-03-2002		xx-xx-2002 to xx-xx-2002

4. TITLE AND SUBTITLE
Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers and Computer Security Officials
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Guttman, Barbara ;

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
National Institute of Standards Technology
xxxxx, xxxxxxx

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
IATAC
3190 Fairview Park Drive
Falls Church, VA22042

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES
CATALOGERS: Report date and dates covered should be 1992.

14. ABSTRACT
See report.

15. SUBJECT TERMS
IATAC COLLECTION

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Public Release	98	email from Booz Allen Hamilton (IATAC), (blank) lfenster@dtic.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	3/1/1992	Report 3/1/1992

4. TITLE AND SUBTITLE
Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers and Computer Security Officials

5. FUNDING NUMBERS

6. AUTHOR(S)
Guttman, Barbara

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

NIST

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

IATAC
3190 Fairview Park Drive
Falls Church, VA 22042

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

The Computer Security Act of 1987 (Pub. L. 100-235) and Office of Management and Budget Circular A-130 mandate that U.S. Government agencies protect automated information and the resources used to process it (hardware, firmware, and software). OMB Circular A-130 specifically mandates that, as a part of protecting computer systems, agencies incorporate computer security in the system acquisition process. This NIST Special Publication provides guidance for federal procurement initiators, contracting officers, and computer security officials on including computer security in acquisitions.To accomplish this goal, computer security and federal information processing (FIP) procurement must be integrated. Computer security is the protection of the integrity, availability and confidentiality of automated information and

14. SUBJECT TERMS
IATAC Collection, information security, computer security

15. NUMBER OF PAGES
97

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

TABLE OF CONTENTS

APPENDICES

LIST OF FIGURES

(Note: Some of the figures were developed using a non-DOS operating system. Consequently, some figures are not included in this ascii version.)

PREFACE

Computers and information play an increasingly important role in modern society. More people use computers, more information is processed and stored by them, and our nation's dependence on computers continues to grow. Therefore, it is essential to protect computers and the information they contain.

From a practical standpoint, computer viruses, white-collar crime, theft of hardware and software, unauthorized access to data, and damage and destruction of computer systems by people or nature are real threats. Computer security shows its worth in preventing loss or harm. The meaning of terms like "appropriate and cost-effective safeguards" are truly appreciated when explaining how a loss was or was not prevented.

Due to the vital need to protect computer systems, the National Institute of Standards and Technology (NIST) provides standards and guidelines on many aspects of computer security. This document addresses the specific issue of including computer security requirements in federal information processing (FIP) procurements. A NIST-sponsored working group of government and industry representatives in computer security, information management, and FIP procurement helped to develop this document.

Working Group Participants and Contributors

Ronald Brunner	Ronald G. Brunner & Associates
Grace Culver	General Services Administration
Donna Dodson	National Institute of Standards & Technology
Virgil Gibson	Grumman Data Systems/National Security Agency
Daniel Gambel	Grumman Data Systems/National Security Agency
E. Taylor Landrum	Grumman Data Systems
Gerald S. Lang	Department of Veterans Affairs
Victor Marshall	Booz-Allen & Hamilton/National Aeronautics & Space Administration
Gary Morris	ANSER
Gary Oran	Federal Emergency Management Administration
Nicholas Pantiuk	Grumman Data Systems/National Security Agency
Chiquita Phillips	General Services Administration
Carmen Santos-Logan	Defense Logistics Agency
Philip Sibert	Department of Energy
Edward Simpson	Department of Energy
Ted I. Wells	Patent & Trademark Office
Stephen C. Willett	U.S. Postal Service
John Zobel	International Software Systems/Department of State

The Working Group gratefully acknowledges input from the following people:

Carol E. Bennett	National Aeronautics & Space Administration
Joan Bonk	U.S. Senate
Leonard Clark	National Aeronautics & Space Administration
Lee Conyers	Department of Transportation
Karen Deneroff	Internal Revenue Service
Barbara Estrada	Department of the Treasury
Irene Gilbert	National Institute of Standards & Technology
Paul Lewis	Department of Energy
Harris McGarrah	U.S. Coast Guard
Michelle Moldenhauer	Department of the Treasury
Noel Nazario	National Institute of Standards & Technology
Bill O'Brian	U.S. Navy
Mervyn Stuckey	Bureau of the Census

CHAPTER I

INTRODUCTION

A. REQUIREMENT

The need to provide protection for federal automated information assets has been present since computers were first used. The Office of Management and Budget (OMB) formally established a federal computer security policy in 1978 and updated that policy in OMB Circular A-130, dated December 1985. Congress passed several laws relevant to computer security, including the Computer Security Act of 1987. Both Congress and OMB update and revise federal policies and regulations on computer security. Computer security concepts and practices are discussed in section II.A, Computer Security.

In order to meet these policies and regulations, federal agencies must include computer security considerations in all phases of information resources management. OMB Circular A-130 and the Federal Information Resources Management Regulation (FIRMR) require security specifications for systems acquisitions. In general, including computer security in the acquisition phase results in less expensive and better security than adding security to an operational system. This document provides guidance on including computer security considerations in the acquisition phase of information resources management.

B. SCOPE

This document is intended to help agencies select and acquire cost-effective computer security by explaining how to include computer security requirements in federal information processing (FIP) procurements. The guideline has three parts. The first part is an introduction to the two disciplines:

- computer security (targeted for FIP procurement personnel); and
- FIP procurement (targeted for computer security personnel).

These overviews provide sufficient knowledge to understand the legal, conceptual, and regulatory underpinnings of the document. It should not be used as a sole guide to computer security or FIP procurement.

The second part explains the integration of computer security into the FIP procurement process. The guideline recommends that the following analyses be included in procurement documentation:

- sensitivity determination;
- analysis of integrity, availability, and confidentiality requirements;
- analysis of level of assurance required; and
- planning phase risk analysis.

The guideline also provides assistance on the selection of computer security features, assurances, and procedures. The guideline clarifies:

- what sources of features, assurances, and procedures are required to be used by law or regulation; and
- what other sources are available and how to use them.

The third part of the document includes specifications and contract language for specific computer security features, assurances, and procedures that can be included in FIP procurements.

This document does not address the procurement of computer security-related services, such as the development of risk analyses and contingency plans. NIST has prepared a separate document, NISTIR 4749, Sample Statements of Work for Federal Computer Security Services, to address procurement of these services.

This document is not a substitute for agency procurement or security regulations, policy, and guidance. It is intended to be used in conjunction with these agency regulations. This document does not address computer security requirements for national security or Warner Amendment information resources.

C. TARGET AUDIENCE

This document targets procurement initiators (the sponsor, program manager, or person who will become the contracting officer's technical representative), contracting officers, and computer security officials.

D. TERMINOLOGY

The terms computer, computer system, automatic data processing (ADP), automatic data processing equipment (ADPE), federal information processing (FIP) resource, information technology support (ITS), information resources (IR), and automated information system (AIS) are used interchangeably throughout the government. In this document, the term FIP procurement is used because it is the term used in the FIRMR, and the term computer security is used because it is the most common. Both FIP procurement and computer security address the resources and services used to enter, store, process, and transmit automated information and data.

Appendix D contains a glossary of selected computer security and procurement terms.

CHAPTER II

BACKGROUND

This chapter provides a general introduction to computer security and FIP procurement. The section on computer security is targeted for contracting officers. The section on FIP procurement is targeted for computer security officials. The sections are not complete step-by-step procedures, but provide background for the rest of the guideline.

A. COMPUTER SECURITY

Computer security is the protection of the integrity, availability and, if needed, confidentiality of automated information and the resources used to enter, store, process, and communicate it. Computer security is often referred to in conjunction with system trustworthiness, integrity, safety, availability, and reliability. In the federal government, the primary policy mandates for protecting computer assets are in OMB Circular A-130, "Management of Federal Information Resources," specifically Appendix III, "Security of Federal Automated Information Systems," and the Computer Security Act of 1987.

This section addresses basic computer security concepts and practices, based on OMB Circular A-130 and the Computer Security Act. Understanding these concepts and practices helps procurement initiators and contracting officers properly integrate computer security considerations into procurements.

A.1. BASIC COMPUTER SECURITY CONCEPTS

Several basic concepts in computer security are described below:

Management Issue. Computer security is an increasingly important issue for all federal managers. Modern technology allows federal agencies to store and process vast amounts of data in support of agency functions. Federal computer and information assets have great value and need to be managed to the same extent as the more traditional organizational assets (i.e., employees, money, equipment, natural resources, and time).

Value of Information and Computing Resources. The value of federal information and computing resources and the importance of federal agency missions create a need for these resources to be adequately protected. Owners and users of the information provide the impetus for protecting these valuable resources.

Functional Requirement. Computer security is a functional requirement of most systems. If data is not accurate, complete, timely, available, and, if necessary, confidential, then the system may be unable to perform its basic function.

Individual Privacy. Automated information about individuals must be protected in accordance with the Privacy Act of 1974 and other statutes.

Life Cycle Phases. Many systems are designed, developed, and implemented over months or years. A system life cycle is used to manage a system from its inception through its development, implementation, and operation until its

termination. If security is initially designed into a computer system, the safeguard options are vastly increased and the security costs over the life of the system are substantially reduced. Since the system environment and technology may change during the system life cycle, the security will need to change also. Therefore, it is important for all managers to ensure that security is appropriately addressed in all phases of the life cycle for computer systems, especially in the early planning stages.

Some automated systems are acquired "off-the-shelf" and can be used immediately. In procuring these systems, initiators must consider the systems' present security features and expandability to meet future security needs. Many vendors offer security features on off-the-shelf systems which may be ordered separately and installed after the system is in operation.

Computer Security Incidents. In recent years federal agencies have become aware of more computer security incidents. These incidents result from intentional and unintentional actions by internal (government and contractor) personnel and outsiders. These incidents result in monetary losses and decrease an agency's productivity and even its ability to perform its mission. While advances in computer and telecommunications technology help prevent many problems, the difficulty of managing the rapid change and the technical complexity can increase the federal government's vulnerability to incidents.

Balance. Absolute security is virtually impossible. Federal agencies cannot totally protect their computer systems from every possible threat for numerous reasons, including the following:

- Absolute protection would make the agency's systems virtually inaccessible and unusable;

- Some vulnerabilities may not be known, as in the case where application code contains security flaws; and

- Computer security, like other disciplines, depends on people, who are capable of error and dishonesty.

Goal. The goal of federal computer security is to support the mission of the agency by providing cost-effective protection that assures the integrity, availability, and confidentiality of automated information and the resources used to process it. There are few clear rules for accomplishing this goal. Nevertheless, OMB Circular A-130 requires that the following types of protective measures be used, alone or in combination, to cost-effectively provide appropriate protection:

- Technical;
- Personnel;
- Administrative;
- Environmental; and
- Telecommunications.

Figure 1 shows how protective measures, called safeguards, are used to protect assets from threats. These safeguards can be internal or external to the system. A threat is any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification, and/or denial of service. If a safeguard is missing or inadequate, a threat can "get through" and damage assets. The damage to the asset has an impact on the agency. The "gap" between the safeguards is referred to as a vulnerability.

The selection of safeguards for a specific computing environment is based on an assessment of the assets, impacts, threats, probabilities, vulnerabilities and the adequacy, availability, and cost of safeguards. This process is called risk analysis.

Figure 1. Threats, Safeguards, Vulnerabilities, & Assets.

Multidisciplinary Coordination. All traditional management disciplines and functions must be employed in a coordinated fashion to effectively manage computer security. Over the years, federal agencies have become more dependent on automation technologies to support all aspects of their operations and missions. As a result, there are many security-related disciplines, each with its own set of policies and procedures.

Figure 2 shows possible functional areas in an agency with responsibilities that overlap with computer security. Many of these are separate career fields within the government. Only when all disciplines are working together, in a highly coordinated fashion, can the entire security process function properly and efficiently. Thus, computer security managers at all levels must regularly coordinate with personnel in other security-related disciplines.

Figure 2. Multidisciplinary Coordination.

A.2. BASIC COMPUTER SECURITY PRACTICES

In practice, certain basic actions are necessary in all federal computer security programs. These include:

Develop Computer Security Policy/Procedures. Computer security policies and procedures are needed to define the overall framework for implementing and sustaining an efficient and cost-effective computer security program at the federal agency level. The policy establishes lines of authority, roles and responsibilities, and basic principles and requirements which define the computer security program. The procedures contain implementation and compliance instructions and management processes.

Institute Computer Security Planning. Computer security planning must provide a consistent approach for determining short- and long-range management objectives, developing security enhancement proposals, mapping proposals to budget requests, and assuring the implementation of cost-effective protective measures.

Institute a Sensitivity Identification Process. The Computer Security Act requires that agencies identify sensitive systems. In order to accomplish this, agencies must institute a process for determining sensitivity.

Define and Implement a Risk Analysis Program. This program should ensure the performance of risk analyses on agency systems. Federal managers need to continually identify and analyze potential threats to their computing and telecommunications environments and take action to reduce risk exposures to acceptable levels.

Establish a Protective Measure Baseline. There are numerous combinations of technical, personnel, administrative, environmental, and telecommunications protective measures available to federal managers. While OMB Circular A-130 defines a governmentwide security baseline, an organization-specific security baseline can help an agency ensure adequate protection of resources.

Ensure the Conduct of Certifications and/or Accreditations. Computer security certifications and/or accreditations are a management control for ensuring that installed security safeguards are adequate.

Oversee a Multi-layer Compliance Assurance Mechanism. Management and compliance reviews should be conducted periodically to sustain optimal security levels.

Develop an Incident Response and Reporting Mechanism. Agencies should develop appropriate responses to security incidents and provide feedback information to senior management on significant incidents. This reporting also supports the tracking of agencywide trends.

Ensure Continuous Awareness and Training. Continuous awareness and training are necessary to elevate and sustain management and personnel awareness and to provide specific guidance for personnel who design, implement, use, or maintain computer systems.

Ensure Contingency Planning. Contingency, disaster recovery, and continuity of operations plans provide continued processing capability when other safeguards have failed to maintain system reliability or availability. Such plans should be in place and tested periodically.

Ensure Personnel Screening. Personnel who participate in managing, using, designing, developing, operating, or maintaining computer systems should be appropriately screened. The level of screening should be commensurate with the loss or harm that could be caused by these individuals. This applies to both federal and contractor personnel. The Office of Personnel Management defines screening requirements for federal personnel.

Develop Appropriate Acquisition Requirements. In contracts for hardware, software, and computer-related services, federal agencies must ensure that:

- appropriate security requirements and specifications are included in statements of work; and

- security requirements and specifications are implemented properly before the system goes into operation.

B. FIP PROCUREMENT

This section provides a general introduction to FIP procurement for computer security officials. The section is not a complete "how to" but provides background for the rest of the guideline.

The acquisition of federal information processing (FIP) resources has discrete characteristics that distinguish it from the acquisition of other supplies or services. FIP acquisitions have unique authority, approval, and documentation requirements. These requirements flow from various laws and are implemented in two primary regulations:

- Federal Acquisition Regulation (FAR); and
- Federal Information Resources Management Regulation (FIRMR).

FIP procurement, as defined by the Brooks Act, the Paperwork Reduction Reauthorization Act, and the FIRMR, involves the acquisition of computer hardware, software, firmware and related services including telecommunications and support services.

The FIRMR is the primary regulation for use by federal or executive agencies in their management, acquisition, and use of information processing resources. It is issued by the General Services Administration (GSA), which has primary responsibility for the management of FIP resources in the federal government.

Note: This section, like the rest of the document, does not address national security systems or systems covered by the Warner Amendment. (See glossary for a definition of Warner Amendment systems.)

The following sections address FIP procurement concepts and practices.

B.1. BASIC PROCUREMENT CONCEPTS

It is essential to have a basic understanding of the underlying goals and objectives of the government's procurement procedures. Without this understanding, the procurement process can be confusing and its rules can appear intractable and obscure. Under these conditions, it is difficult to

include computer security. In addition, because conflicts and problems sometimes arise during a procurement, knowledge of the underlying goals and objectives will help the procurement initiator work with the procurement staff to resolve problems.

The following analysis is a basic tutorial on the essential elements of federal government procurement. It is not intended to substitute for the FAR, the FIRMR, or your agency's procurement guidelines.

Federal procurement is governed by its underlying goals. These goals are:

- to obtain quality products that meet the government's needs at the best price (now and in the future);

- to promote innovation and growth in American industry; and

- to promote the social and economic development of certain segments of American society.

The government attempts to meets its goals with certain objectives. These objectives are derived from the goals and the fundamental nature of how the government operates. The objectives are:

- Competition. The government recognizes that competition causes offerors to lower price and increase quality in order to win contracts. Competition is the primary means of attaining economy and efficiency in satisfying the needs of the government. The government recognizes that new sources must be considered to increase the number of options, to stimulate new ideas by providing an accessible market, and to be fair to all businesses interested in selling to the government.

- Fairness. In order to achieve meaningful competition, the government must conduct procurements fairly. By offering all vendors and new ideas a fair chance, the government encourages growth.

- Promotion of small, minority-owned, woman-owned, and disadvantaged businesses. The government recognizes that the socio-economic development of these groups is to the advantage of the country. This objective is closely related to the previous objective.

Given these diverse goals for the procurement process and the myriad individual situations, it is possible for conflicts to arise in the process.

B.2. BASIC FIP PROCUREMENT PRACTICES

The administration of these goals and objectives in FIP procurement is governed by laws and regulations which are implemented in the FAR, the FIRMR, and agency regulations. While these sources contain much more information, the following is a brief list of fundamental practices.

GSA Responsibility. GSA has authority for the management and oversight of FIP procurement. Agencies, however, are responsible for defining their requirements. GSA exercises its authority in a number of ways:

Delegation of Procurement Authority (DPA). GSA exercises its authority through the use of DPAs. Without a DPA, an agency cannot acquire FIP

resources. There are three types of delegations: regulatory, specific agency, and specific acquisition. GSA can withdraw or limit DPAs and can refuse to grant DPAs until procurements conform to GSA standards.

GSA Reviews. GSA conducts periodic reviews to assess how agencies are acquiring and managing FIP resources.

General Services Board of Contract Appeals (GSBCA). The GSBCA was created by the Competition in Contracting Act of 1984 to hear protests relating to FIP procurement. (Contract cases can also be heard by the General Accounting Office, the procuring agency, or the courts.) The GSBCA can uphold or overturn procurements and can suspend an agency's DPA.

Vendors can protest a specification or action of the government relating to a particular procurement if the protest meets certain administrative and legal constraints. Vendors can protest that a specification is restrictive, that the agency does not require a certain specification, or that the government was unfair or did not follow its procedures correctly. The protesting of specifications has caused the government to not only identify requirements, but also justify them.

A protest can delay a procurement for months or years and can result in an agency having to amend the solicitation or, in a worse case, issue a new solicitation. A solicitation that is well justified by the supporting documentation is essential to minimize protests and to lessen their duration.

Full and Open Competition. The Competition in Contracting Act of 1984 requires the government to use full and open competition. Sometimes procurement initiators are confused about the definition of full and open competition. Full and open competition is achieved when all responsible sources are given the opportunity to submit a proposal and be considered.

Full and open competition is not necessarily achieved when there is more than one source. Consideration of three products does not mean that the government can refuse to consider a fourth responsible source. The government must consider products from all responsive and responsible sources. (See glossary for definitions of responsive and responsible.)

Note: There are exceptions to full and open competition that are described in FAR 6.3.

B.3. PROCUREMENT CYCLE FROM THE PROCUREMENT INITIATOR'S POINT OF VIEW

The procurement initiator is the sponsor or program manager who represents the organization that needs the FIP resources. This person often becomes the contracting officer's (technical) representative (COR or COTR) after award. The procurement cycle is the progression of stages in the process of acquiring property or services. From the procurement initiator's point of view, the procurement cycle consists of four stages: planning, solicitation, source selection, and contract administration and closeout.

Planning. Procurement planning can be divided into two subsections: general planning and the specific planning for a procurement. Part 7 of the FAR provides additional guidance on acquisition planning.

Solicitation. Solicitation refers to the process of asking vendors for proposals (also called offers) or bids. This guideline addresses the Request for Proposals (RFP) because it is the most common and most complex form of solicitation. There are other methods, such as the Invitation for Bids (IFB) or Request for Quotes (RFQ). The ideas in this guideline can be used for all types of solicitations.

An RFP has 13 sections, which are generally referred to by letter. Figure 3 lists the sections. Appendix A contains a chart describing the sections.

Letter	Section Title
A	Solicitation/Contract Form - Standard Form 33
B	Supplies or Services and Prices and Costs
C	Descriptions/Specifications/Work Statement
D	Packaging and Marking
E	Inspection and Acceptance
F	Deliveries or Performance
G	Contract Administration Data
H	Special Contract Requirements
I	Contract Clauses
J	List of Attachments
K	Representations, Certifications, and Other Statements of Offerors or Quoters
L	Instructions, Conditions, and Notices to Offerors
M	Evaluation Factors for Award

Figure 3. RFP Sections.

Source Selection. Source selection is the process of evaluating offers against criteria stated in the solicitation and selecting the offer that best meets the government's requirements. Source selection can involve various forms of interactions with offerors including negotiations, clarification requests, discussions, and best and final offers (BAFOs). It can also include performance and capability testing. In addition, the government must notify unsuccessful offerors and debrief them, if requested.

Contract Administration and Closeout. Contract administration refers to the management of the contract, including inspection and acceptance of deliverables and modification of the contract. It occurs after actual contract award. Contract administration duties are shared by the contracting officer and the contracting officer's technical representative (COTR). Closeout is the action that is taken when performance under the contract is completed.

Procurement Cycle Figure. A figure showing the FIP procurement cycle from the procurement initiator's point of view is presented in figure 4. Chapter three will expand on the figure by incorporating computer security activities. Procurement initiators who are unfamiliar with the procurement cycle should obtain additional guidance from their procurement office.

Many of the actions taken by the contracting officer are not reflected in this figure.

PROCUREMENT CYCLE

FROM THE PROCUREMENT INITIATOR'S POINT OF VIEW

Planning		Solicitation	Source	Adminis-
General	Procurement Specific		Selection	tration & Closeout
Strategic/ Tactical Planning	Requirements Analysis	Statement of Work	Evaluation of Proposals	Inspection & Acceptance
Needs Determination	Analysis of Technical Alternatives	Evaluation Plan		COTR Responsi- bilities
	Feasibility Study	Review of Solicitation		
	Cost/Benefit Analysis			
	Software Conversion Study			
	Market Study			

Figure 4. Procurement Cycle.

CHAPTER III

INCORPORATING COMPUTER SECURITY INTO THE PROCUREMENT CYCLE

To effectively include computer security in the procurement process it must be integrated into the procurement cycle from its inception. This guideline focuses on the computer security components of the procurement cycle. Sufficient information about the procurement cycle is included to allow a person not familiar with the procurement process to understand the chapter. This chapter does not provide a complete description of the procurement process. (See the FAR and the FIRMR for detailed procurement information.)

A. PARTICIPANTS

There are many participants who can have a computer security or oversight role in procurements depending on the nature and scope of the system. These participants are listed both by type of role and by functional title. The names for the roles and titles will vary in different organizations. Each of these does not necessarily provide input in every phase. For instance, support contractors and vendors are restricted from participating in some phases. The determination of which participants need to be consulted is as unique as the procurement.

The list of participating groups and offices below is not all inclusive, but does represent many of the functions that can impact security.

Procurement Initiator/Sponsor
Functional Manager/Owner of data
Users
Procurement/Contracts
Certification/Accreditation
Computer Security
Quality Assurance/Quality Control/Safety
Legal
Information Resources Management
Design/Engineering
Budget
Audit/Internal Control
Physical/Personnel Security
Facilities/Logistics
Support Contractors/Consultants
Manufacturers/Suppliers/Vendors

The length of the list is indicative of the difficulty of managing and acquiring FIP resources. It is vital that these groups work together to ensure that important aspects of the procurement are addressed.

As with any acquisition, it is important to involve the contracting officer as early as possible, preferably in the planning stage.

B. COMPUTER SECURITY IN THE PROCUREMENT CYCLE

The purpose of this section is to define steps that will integrate computer security into the procurement cycle. The section explains each of the

computer security steps of each phase of the procurement cycle. During the procurement cycle, the technical and security requirements will be advanced together.

Figure 6, Computer Security in the Procurement Cycle, located at the end of this chapter, illustrates how security fits into the procurement cycle. It expands on figure 4 in chapter two and maps security-related activities to the procurement activities already being performed. This chapter will explain each computer security activity in figure 6.

The computer security steps in this section describe analyses and processes to be accomplished. These steps define a conceptual framework for computer security planning during the procurement cycle. This framework is intended to be used as an example; it is not a definitive methodology. The framework contains descriptions of a core set of planning considerations that will lead to the production of computer security acquisition specifications, as required by OMB Circular A-130. Agencies can use other methodologies or modify the one presented here.

B.1. PLANNING

The first phase in the procurement cycle is planning. Planning is normally divided into General Planning and Procurement Specific Planning. General planning involves planning on an organizational level. This section addresses the needs determination component of general planning. Procurement specific planning involves planning for a specific system or acquisition. In this document, procurement specific planning is further broken down into the Requirements Analysis and Other Planning Components.

B.1.a. Needs Determination

The needs determination is an initial definition of a problem that might be solved through automation. It is also called a requirements determination. Traditional components of the needs determination are a basic system idea, a preliminary requirements definition, feasibility assessment, technology assessment, and some form of approval to further investigate the problem.

A need may have been determined from strategic or tactical planning. The following definitions are from the GSA publication Acquisition of Information Resources: Overview Guide.

> Strategic planning defines the major information resources activities and types of information required by the organization and produces a high-level strategy for pursuing the organization's information resource needs.
>
> Tactical planning is the identification, scheduling, management, and control of tasks necessary to accomplish individual activities identified in the strategic plan.

Acquisition planning can only begin after an agency has determined that a need exists. The needs determination phase is very high-level in terms of functionality. No specifics of a system are defined here. The idea for a new or substantially upgraded system and the feasibility of the idea are explored. During this early phase of the acquisition, the definition of the security requirement should begin with the preliminary sensitivity assessment.

Preliminary sensitivity assessment. The preliminary sensitivity assessment should result in a brief qualitative description of the basic security needs of the system. These should be expressed in terms of the need for integrity, availability, and confidentiality.

This does not require an elaborate sensitivity analysis scheme, but does require an assessment of the significance of the systems. Legal implications, federal policy, agency policy, and the functional needs of the system help determine its sensitivity. Factors including the importance of the system to the agency mission and the consequences of unauthorized modification, unauthorized disclosure, or unavailability of the system or data should be considered when assessing sensitivity.

B.1.b. Requirements Analysis

The requirements analysis is an indepth study of the need. It draws on the work done during the needs determination and develops it. Requirements analyses are required by FIRMR Part 201-20.102:

> Agencies shall establish and document requirements for FIP (federal information processing) resources by conducting a requirements analysis commensurate with the size and complexity of the need.

The following computer security components should be included in a requirements analysis:

- Analysis of integrity, availability, and confidentiality requirements;
- Update sensitivity assessment;
- Analysis of the level of assurance required;
- Planning phase risk analysis; and
- Preliminary certification/accreditation plan.

As stated above, these analyses present a conceptual framework for computer security planning. They are intended to be used as a guide, example, or roadmap. Other methods of computer security planning are acceptable.

While this section presents the computer security components of the requirements analysis in sequential fashion, they can be done in a different order. For more complex systems, they will need to be done cyclically until all of the components work together. For smaller acquisitions, all of the components can be combined into one analysis. Figure 5 at the end of this section shows how the computer security components of the requirements analysis phase can interact.

Analysis of integrity, availability, and confidentiality requirements. Computer security is defined as the process for determining, cost-justifying, and applying the technological safeguards and managerial procedures to protect information processing resources, including data, hardware, software, telecommunications, and related services. In practice, the need for protection is expressed in terms of the need for integrity, availability, and confidentiality. Integrity can be looked at from several perspectives. From a user's or application owner's perspective, integrity is a quality of data that is based on attributes such as accuracy and completeness. From a systems or operations perspective, integrity is the quality of data that it is only

changed in an authorized manner or that the system/software/process does what it is supposed to do and nothing more. Like integrity, availability also has a multi-part definition. Availability is the state when data or a system is in the place needed by the user, at the time the user needs it, and in the form needed by the user. Confidentiality is the privacy, secrecy, or nondisclosure of information except to authorized individuals.

The first step in the analysis is to determine what the protection requirements are. The analysis will be built upon the sensitivity assessment done during the needs determination, but will be more indepth and specific.

This process should include an analysis of laws and regulations such as the Privacy Act, the Federal Manager's Financial Integrity Act, the Computer Security Act, OMB circulars, agency enabling acts, and other legislation and federal regulations which define baseline security requirements. After a review of mandated requirements, agencies should consider functional and other security requirements.

At this level, as opposed to the needs determination level, the analysis should be system specific. The legal, functional, and other computer security requirements should be stated in specific terms. For complex systems, this will require more than one iteration of the requirements analysis components.

Since most systems have at least minimal integrity and availability requirements, care should be taken to address these areas clearly. Computer security is more than confidentiality. Even systems with no confidentiality requirement need security to meet integrity and availability requirements.

Update Sensitivity Assessment. After completing the analysis of integrity, availability, and confidentiality requirements, the sensitivity assessment should be updated based on the results.

Analysis of the level of assurance required. The correct and effective use of computer security controls is a fundamental building block of system security. Assurance is the degree to which the purchaser of a system knows that the security features and procedures being acquired will operate correctly and will be effective in the purchaser's environment.

Obtaining assurance can be quite difficult because assurance can be expensive and can be hard to quantify. This analysis needs to address how much confidence is needed that the computer security will work correctly and effectively. The analysis should be based on both legal and functional requirements and will be the basis for determining how much and what kinds of assurance are required. This assurance analysis will lead directly to the evaluation plan which will be developed in the solicitation phase. It can also be used to help determine appropriate acceptance criteria.

As with other aspects of security, it is important to remember that the goal is cost-effective security, not absolute security. Absolute security is virtually impossible to attain and can be cost prohibitive in terms of system usefulness and dollars.

There are many techniques for obtaining assurance. For a further discussion, including a list of assurance methods, see Appendix B.

Review by Other Functional Groups. Depending on the size and scope of the system, a team or group of participants from the functional groups described

in the beginning of this chapter may be useful. Even for small systems, it may be helpful to get the assistance of the computer security staff. These functional groups may have insight into the integrity, availability, confidentiality and assurance requirements. Getting these groups involved early in the planning process is important since it may result in reduced life cycle cost because it is easier to change requirements in the early stages.

Planning Phase Risk Analysis. The planning phase risk analysis is a critical step. It is used to determine what types of controls will be cost-effective and forms the basis for determining mandatory and desirable specifications. OMB Circular A-130 requires a risk analysis prior to the approval of design specifications. In addition, a risk analysis can provide justification in case specifications are protested.
The planning phase risk analysis will not necessarily be a large and complex document. The analysis, like other risk analyses, should consider assets, threats to the assets, potential vulnerabilities, and what can be done to reduce vulnerabilities. The planning phase risk analysis should take into consideration what controls already exist and their effectiveness. The planning phase risk analysis will probably require participation by the other functional groups.

The planning phase risk analysis will use input from the analysis of integrity, availability, and confidentiality requirements as the basis for determining the value of information assets and the impact of security failures. The selection of appropriate types of safeguards should take into consideration the results of the level of assurance analysis. The planning phase risk analysis, in turn, may point out deficiencies in the analysis of integrity, availability and confidentiality requirements or the level of assurance analysis by demonstrating the logical conclusion of the analyses.

Further information on the planning phase risk analysis is contained in Appendix C.

Review by certification and/or accreditation official. OMB Circular A-130 requires that systems be approved for processing based on the adequacy of the safeguards. This process is referred to as both certification and accreditation in different agencies. The approval is made by either the program manager or a designated approving official. Since this official has responsibility for accepting the risk, it is prudent to get approval of the certification and/or accreditation approach. The certification and/or accreditation approach should address the vulnerabilities that may exist in the system. The approving authority can advise the acquisition team if the risks appear to be acceptable. It is easier to incorporate requirement changes during the planning stage of a system acquisition than during the solicitation, source selection, or contract administration stages.

The acquisition team and the approving authority should also discuss what forms of assurance the approving authority needs to make a decision. This can include system tests and other items that need to be addressed in the solicitation. Assurance is discussed in Appendix B.

In addition, the procurement initiator and the approving authority should discuss how changes to the system and its environment will be addressed. The possibility of a security working group should be discussed. The group can consist of various types of people such as application sponsors; system, security, or database administrators; security officers or specialists; and system or application analysts. Section IV.F presents specifications for this

group.

For further information on certification and accreditation see FIPS PUB 102 Guideline for Computer Security Certification and Accreditation.

Cyclical Nature of the Process. As stated in the introduction, these requirements analysis sub-components may need to be performed cyclically. The components inter-relate and build on each other. Depending on the size and complexity of the system, these components may be performed many times as ideas become refined and focused. The flow model on the next page (fig 5) shows how the computer security components of the requirements analysis phase of the procurement cycle can work together.

Figure 5. Flow Model for Computer Security Components.

B.1.c. Other Planning Components

There are several other parts of the planning process that will incorporate computer security in their cycles:

- feasibility study,
- system cost-benefit analysis,
- software conversion study,
- analysis of technical alternatives, and
- market surveys.

The feasibility study should also look at the computer security of the system. If security is not considered during the feasibility study, then it is possible for a computer system to be acquired for which there is no cost-effective security solution.

The cost-benefit analysis should use input from the planning phase risk analysis. If the cost-benefit analysis does not consider security, then it is possible for it to favor a system which will later require security upgrades (which could be expensive). In addition, it could favor a system with unnecessary exposures to traumatic failures.

The software conversion study, which examines the cost of re-establishing software on a new hardware or software base, should include the cost of re-establishing the desired degree of computer security on the new system and maintaining security during the transition.

The analysis of technical alternatives should rate the alternatives against their ability to meet all the requirements including computer security.

The market surveys, which may include Requests for Comment (RFCs) or Requests for Information (RFIs), should include the computer security requirements.

At the end of the planning phase, the government will have determined the requirements and the best ways to achieve them. This will include a decision on whether a requirement can be met through acquisition or in-house development. Many systems combine these methods. Since the planning phase looks at the whole system, the computer security and other functional requirements should have been adequately addressed to allow acquisition of components while maintaining system integrity.

Many agencies have an approval process, which may include computer security, at the end of the planning phase. The approval can be used to see if the procurement incorporates a rational risk-based approach to security planning. (It is not necessary for the procurement initiator to have exactly followed the steps outlined in this special publication; other approaches can be used.)

B.2. SOLICITATION

The second phase in the procurement cycle is the solicitation phase. This covers the development and issuance of the request for proposals (RFP) and the receipt of proposals.

All considerations surrounding the acquisition of the product or service must be addressed in the solicitation. This includes the description of what is being acquired; how it will be acquired; how it will be evaluated, tested, and

accepted; and how the contract will be administered. Although the actual evaluation of proposals or the administration of the contract happens in later phases, these areas must be addressed now.

An RFP is designed to allow the government to make a best value decision based on an offeror's proposal. One of the strengths of the RFP process is the flexibility it provides the government and the offeror to negotiate a contract that best meets the government's needs.

The government can identify needed computer security features, procedures, and assurances in many ways. An RFP can be a flexible document which allows for substantial creativity. Guidance on procurement alternatives should be obtained from the agency procurement office or the contracting officer.

Because of the flexibility, it is impossible to address precise mapping of the computer security considerations into the uniform solicitation. The procurement initiator needs to decide how the computer security considerations will be met given the many options an RFP provides.

This guideline explains some of the considerations for developing a statement of work/specification and provides general guidance about evaluation, testing, and acceptance of the computer security features. The procurement initiator must decide how a given feature, procedure, or assurance fits in the RFP. In addition, this guideline provides guidance about clauses.

B.2.a. Specifications and Work

The statement of work (SOW) or specification is based on the requirements analysis. This section describes two types of sources for computer security specifications: general specifications and federally mandated specifications.

Security requirements can be included in the SOW as specifications, tasks, labor, work, level of effort, etc. The procurement initiator should concentrate on what is required and work with the contracting officer to determine how to ask for it.

General Specifications

There are many sources of general computer security specifications. NIST guidance documents, such as this one, and guidance from other federal agencies and commercial groups are some sources. The indexes to NIST documents are referenced below and are updated periodically. Also, DoD has extensive material that can be used for guidance. The Trusted Computer Systems Evaluation Criteria (TCSEC) or "Orange Book" is a DoD standard that defines many computer security specifications. The TCSEC is a DoD standard but NOT a federal government standard. There are also specifications in other DoD and other agency computer security guidelines. Commercial sources and trade organizations also publish general computer security specifications.

These computer security documents can be reviewed for applicability to the system(s) being procured. They may represent areas that were overlooked and they can save time since they provide already prepared SOW language. Care should be taken when selecting features, procedures, and assurances from these sources. The items may be grouped based on interdependencies between the items. It is necessary to understand the features, procedures, assurances,

and groupings before specifying them separately.

Each specification must be justified from the requirements analysis, specifically from the planning phase risk analysis. Safeguards recommended by a general source should be considered, but they should not be included in an RFP if the risk analysis does not support them.

Federally Mandated Specifications

There are other sources of computer security (and nonsecurity) specifications which are required by law to be included in the RFP. These are often referred to as directed specifications. All federal agencies must require that systems comply with applicable FIPS PUBS and Federal Standards. Executive agencies must comply with OMB Circular A-130. There are also agency-specific directed specifications, which are official policies issued with the concurrence of agency legal and procurement officials.

Directed specifications must be incorporated in an RFP if the system being acquired matches the criteria in the directed specification. It is very important to be aware of directed specifications. If specifications in an RFP conflict with directed specifications, a waiver must be obtained.

The following publications contain lists of standards including FIPS PUBS and Federal Standards:

- NIST Publications List 58 - Federal Information Processing Standards Publications (FIPS PUBS) Index
- NIST Publication List 88 - Computer Systems Publications
- NIST Publications List 91 - Computer Security Publications
- GSA Handbook "Federal ADP and Telecommunications Standards Index"

Ordering information for NIST publications is printed on the inside back cover of this document. The GSA Handbook is available from the Government Printing Office.

Another source for directed specifications is the Model Framework for Management Control Over Automated Information Systems published jointly by the President's Council on Management Improvement and President's Council on Integrity and Efficiency. This document provides guidance on requirements for control imposed by the Federal Manager's Financial Integrity Act of 1982, the Privacy Act of 1974, and OMB Circulars A-123, A-127, and A-130. The Framework states, "...federal managers are expected to:

- Understand the 55 control requirements identified in the report; and
- Implement a program that demonstrates compliance with the requirements."

It is incumbent on the procurement initiator to know what federal standards apply to the system(s) being procured. Many people erroneously feel that this is the responsibility of the contracting officer. These are technical issues and are, therefore, the responsibility of the procurement initiator.

B.2.b. Evaluation

Evaluation is the process of determining if an offer meets the minimum requirements described in the RFP and an assessment of the offeror's ability to successfully accomplish the prospective contract. This involves a technical analysis of the merits of a proposal. As part of the solicitation phase, the procurement initiator, working with the contracting officer,

develops an evaluation plan to determine the basis for the evaluation and how it will be conducted. The evaluation itself is performed during the source selection phase of the procurement.

Developing an Evaluation Plan.

When evaluating computer security features, it can be difficult to assess if the offer meets the minimum requirements or can successfully accomplish the prospective contract. Therefore, offerors should have to provide assurance to the government that hardware and software claims regarding computer security features are true and that the offeror can provide the proposed services. Since computer security, like other parts of computer systems, is a complex and important subject, the offeror's assertions may not provide sufficient assurance. Appendix B further discusses assurance and presents ideas for how the government can obtain it. In addition, section IV.D provides descriptions of documentation that can be used for assurance in the evaluation phase, such as the offeror's strategy for security.

How assurances are provided may, in fact, determine the ability of the government to adequately assess them. Security personnel need to be sure they are asking for the information they really need. If, after award, the government determines that more assurance is required, the government may be liable for additional costs.

The determination of how the offerors will be required to provide assurance should be considered when developing the evaluation plan. This plan will be used to help develop sections of the RFP which provide instructions to the offerors and information about how the proposals will be evaluated and how source selection will be performed.

As part of this process, a determination of security acceptance testing should be made. It may be important to coordinate evaluation and acceptance to effectively manage the security review and testing of proposals and deliverables.

Items to Consider in the Evaluation Plan.

The remainder of this section presents ideas to assist with the development of the computer security aspects of the evaluation plan. One aspect of the evaluation plan is selecting evaluation team members. Section III.B.3, Source Selection, discusses some of the roles and duties of the evaluation team.

When the evaluation plan is developed, keep in mind that alternatives may conflict with each other. For example, features which provide computer security can conflict with those that provide ease of use. The government must make it clear how offerors should propose different configurations and present conflicting options and trade-offs. However, care should be taken to keep proposal size manageable to facilitate review and to keep proposal preparation costs down.

When computer security is important in the acquisition, it must be addressed in the evaluation criteria so that offerors will know that it is important to the government. Offerors look at the RFP to determine what the government considers most important.

Testing is one method of determining if the proposed system or product can meet the computer security requirements. Depending on the nature of the

system, this can be part of the proposal evaluation, in the form of live test demonstrations or benchmarks, or it can be part of post-award acceptance testing. During the evaluation process there are different times when the testing can occur. There are cost, technical, and procurement integrity considerations for deciding when testing is done. In general, expensive tests should be kept to a minimum. This will help control offeror proposal preparation costs. Not only do expensive proposals limit competition, but the costs are ultimately passed to the government in higher contract costs. Guidance on testing alternatives should be obtained from the contracting officer.

Note: Be sure the computer system testing, especially performance testing, is done with the computer security features enabled.

Warning: The more the procurement initiator knows about the market place, the easier it is to develop an evaluation plan. Proposals cannot be used for market research. The evaluation plan virtually cannot be changed after the receipt of proposals. Additional knowledge learned by reading proposals cannot be used to modify the evaluation plan. It is worth the time to research what kind of alternatives could be offered so a scheme that reflects the true priorities of the government can be developed.

B.2.c. Special Contract Requirements

There are elements in an RFP that are computer security-related but are not contained in the statement of work or the evaluation criteria. These elements usually address rights, responsibilities, and remedies assigned to the parties of the contract. Many times such obligations survive the actual performance period of the contract. Therefore, such elements are best addressed through specific contract clauses or requirements. The nondisclosure of automated information learned during the course of the contract is one example.

Chapter four addresses clauses as well as statement of work items. The procurement initiator must coordinate with the contracting officer about clauses to be added to an RFP.

B.3. SOURCE SELECTION

Source selection is the determination of the successful offeror. The source selection phase is based on the work done in the planning and solicitation phases. This phase involves actually evaluating the proposals and making best value decisions based on the evaluation criteria and other factors stated in the RFP. Computer security considerations incorporated during the planning and solicitation phases will be a part of the evaluation and source selection.

An individual with extensive computer security expertise should be part of the evaluation team. This expert should be available to review the original proposals as well as clarifications, discussion points, and best and final offers (BAFOs). A good review team is essential to the success of a procurement.

B.4. ADMINISTRATION AND CLOSEOUT

The final phase in the procurement life cycle is administration and closeout.

Computer security issues for administration and closeout should have been addressed when developing the solicitation. Two important computer security functions during this phase are acceptance and monitoring contractor performance.

Acceptance. Acceptance refers to the government's decision to accept, and therefore, pay for a deliverable. The government should be careful in accepting deliverables. Testing by the government or an independent validation and verification (IV&V) contractor to determine that the system does meet specifications can be very useful. This should include testing the security of the system.

Note: Acceptance and approval to operate (certification or accreditation) are related, but different concepts. The government normally accepts a deliverable that meets the specifications in the contract. The approval to operate is a separate decision made based on the risks and advantages of the system. It is incorrect to have the approval to operate as one of the acceptance criteria.

Monitoring. In general, the government should plan to review contractor performance to ensure that security has not degraded and that changes in the environment and system that result in new threats and vulnerabilities are recognized and appropriate safeguards put in place. For more complex contracts including more than just purchase of hardware, a security working group is an effective way to monitor security. Section IV.F provides features, procedures, and assurances related to contract administration and closeout.

After award, the government's requirements should not change. If they do, there are mechanisms to modify the contract to accommodate some changes. However, these modifications can be quite costly. In addition, some changes may require separate procurements. As noted in the introduction to this document, new security controls that are retrofitted to a system may not be as effective as controls designed into the system.

CHAPTER IV

SPECIFICATIONS, CLAUSES, AND TASKS

This chapter provides specifications, tasks, and clauses that can be used in RFPs to acquire computer security features, procedures, and assurances. None of the specifications, tasks, or clauses are mandatory. They are intended as a source of general specifications, as defined in section III.B.2.a. They are written for different types of acquisitions including purchase of off-the-shelf products, purchase of integrated systems, development of applications, and other computer-related services.

The specifications, tasks, and clauses are divided into ten categories. Within each category there may be specifications, tasks, and/or clauses as well as explanations, considerations, and/or prescriptions about their use. The specifications, tasks, and clauses are printed in courier typeface. Explanations, considerations, and prescriptions are in regular type face. None of the specifications, tasks, or clauses should be used blindly. Each of them should be tailored to meet individual circumstances. The categories are:

A. General Computer Security

B. Control of Hardware and Software

C. Control of Information/Data

D. Documentation

E. Legal Issues

F. Contract Administration, End of Task, Closeout

G. Computer Security Training

H. Personnel Security

I. Physical Security

J. Computer Security Features in Systems

A word of caution on the use of subcontractors: Ensure applicable computer security requirements and/or certifications placed on prime contractors are also reflected in subcontracts. This is called "flowdown."

The categories above do not address tasking language for specific security services such as having a risk analysis performed or having contractors prepare security planning documents. Tasking language for these types of services are provided in another NIST report, Sample Statements of Work for Federal Computer Security Services.

A. General Computer Security

In keeping with OMB Circular A-130, Appendix III, security responsibility must be assigned. The responsibility must rest with a government employee. This item should be included to clarify responsibility. If the contract calls for computer security administration, management, or support, the delineation of responsibilities should be clear, with the government person retaining ultimate responsibility.

The person responsible for computer security is _____.

The following can be used to show the relationship between agency ownership of federal information processing (FIP) resources and contractor use. These clauses help establish clear lines of authority and responsibility.

The government authorizes the use of agency computer resources (list specific resources if appropriate) for contractor performance of the effort required by the statement of work of this contract.

The contractor shall comply with the requirements of the agency computer security program as defined by (insert agency handbook, directives, manuals, etc.)

B. Control of Hardware and Software

The government should consider who can introduce hardware and software onto the system and under what circumstances.

Introduction and Change of Software - In order to reduce the chance of viruses and other forms of malicious code, of illegal use of licensed software, and of software that may open security vulnerabilities (such as operating system utilities or untested software updates), consider restricting contractors by using the following types of specifications and tasks. These specifications and tasks could be used when the contractor is providing a service such as running or maintaining a government computer system.

Only licensed software and in-house developed code (including government and contractor developed) shall be used on (system name(s)). No public domain, shareware, or bulletin board software shall be installed unless prior written approval is obtained from the contracting officer or COTR.

The following specification is fairly restrictive. The alternatives which follow can be used to modify the specification.

The only hardware and software packages that shall be used on (system name(s)) is (listed here or specify section). All additional hardware and software packages proposed for use, including upgrades, must be approved in advance and in writing by the contracting officer or COTR.

Alternatives:

The contractor shall provide a list of software and hardware changes _____ working days in advance of installing (or other time or performance period).

The contractor shall provide an impact analysis for proposed hardware and software changes that includes an assessment of possible new security vulnerabilities (include other assessment items required) _____ working days in advance of installing.

The contractor shall provide proposed hardware and software for testing _____ working days in advance of loading.

The contractor shall provide proof of license for new software.

The contractor shall maintain a list of hardware, firmware, and software changes throughout the contract. The contractor shall provide this list to the government (specify time frame and/or at the end of the contract).

If the contractor is using their own software, then the following specification can be used to help protect the government from buying products developed with stolen software.

The contractor shall provide proof of license for all software used to perform under this contract.

The following clauses are reprinted from FIRMR Section 201-39.5202-5, Privacy or Security Safeguards. FIRMR Section 201-39.1001-3 prescribes that these clauses, or variations of them, be used in solicitations and contracts

requiring security of FIP resources or for the design, development, or operation of a system or records using commercial FIP services or support services. Clause (a), which addresses ownership of and rights to developed software, should be coordinated with the contracting officer or legal counsel.

(a) The details of any safeguards that the contractor may design or develop under this contract are the property of the government and shall not be published or disclosed in any manner without the contracting officer's express written consent.

(b) The details of any safeguards that may be revealed to the Contractor by the government in the course of performance under this contract shall not be published or disclosed in any manner without the contracting officer's express written consent.

(c) The government shall be afforded full, free, and uninhibited access to all facilities, installation, technical capabilities, operations, documentation, records, and data bases for the purpose of carrying out a program of inspection to ensure continued efficacy and efficiency of safeguards against threats and hazards to data security, integrity, and confidentiality.

(d) If new or unanticipated threats or hazards are discovered by either the government or the contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party. Mutual agreement shall then be reached on changes or corrections to existing safeguards or institution of new safeguards, with final determination of appropriateness being made by the government. The government's liability is limited to an equitable adjustment of cost for such changes or corrections, and the government shall not be liable for claims of loss of business, damage to reputation, or damages of any other kind arising from discovery of new or unanticipated threats or hazards, or any public or private disclosure thereof.

One option to modify these clauses is to add a task related to clause (d):

The contractor shall provide an analysis of the new threat, hazard, or vulnerability and recommend possible fixes or safeguards.

The following two clauses address other issues in the use of government hardware and software by a contractor providing services. The government should include all restrictions such as single site licensing, proper use to maintain warranties, proprietary code, or special considerations.

Under no circumstances is a contractor permitted to make any use of agency computer equipment or supplies for purposes other than performance on this contract.

The following items of government furnished equipment or software have the following licensing or use restrictions: (provide list)

The special needs of personal computers should be addressed. There are many PC security options such as PC security hardware and software, locks, removable hard drives, and anti-virus software. Consider if these are needed when PCs are acquired or if contractors will be using PCs. Remember that a PC used as a terminal is still a computer.

The contractor shall not allow employees to use files for logging onto systems that contain the employee's passwords.

Pre-logon warning messages can deter unauthorized use, increase computer security awareness, and provide a legal basis for prosecuting unauthorized access. Consider having an installation, support, or integration contractor configure multi-user systems with a warning message. Warning messages can also be used on contractor systems processing federal information.

The system(s) shall be delivered/installed with the following message appearing before logon:

(or)

Contractor multi-user systems used to process data under this contract shall use the following pre-logon warning message:

```
WARNING                    WARNING                    WARNING
************************************************************
THIS COMPUTER IS OPERATED BY/FOR THE U.S. GOVERNMENT.  UNAUTHORIZED ACCESS TO
AND/OR USE OF THIS COMPUTER SYSTEM IS A VIOLATION OF LAW AND PUNISHABLE UNDER
THE PROVISIONS OF 18 USC 1029, 18 USC 1030, AND OTHER APPLICABLE STATUTES.
************************************************************
WARNING                    WARNING                    WARNING
```

Having the contractor provide contingency, continuity of operations, and disaster recovery plans for government systems or for their own systems that process government data is another important issue. The following addresses continuity of operations planning for a mission-essential network, but can be tailored for other types of systems. To use this clause, the offerors must have sufficient information to be able to postulate the types of emergencies that could occur. It may be necessary to provide additional detailed specifications to give offerors and evaluators enough information to prepare/review cost estimates and to make objective evaluations.

Add to Section L:
As part of the proposal, the offeror shall submit a preliminary continuity of operations plan to address the planned reaction to threatened or actual emergencies. Provisions for testing the plan, at the option of the agency, must be included in the proposal.

The offeror shall describe how proposed architecture, technical capabilities and organization will protect the system during emergency situations. The plan should state what priority the agency will have in terms of services, replacement hardware, etc. Examples of how these resources will be brought to bear during an emergency are required.

The offeror shall describe external emergency management interface arrangements that will be used with subcontractors if necessary.

The agency is concerned that service may be degraded in a network environment in which switching systems and transmission channel are shared with others. If the offeror proposes such a shared environment, the offeror must address the following issues:

- protection of critical agency users from access blocking;
- protection of network access ports from saturation caused by other traffic that may be using the network access ports; and
- provision of low delay, low blocking access to all necessary intercity routes and access facilities for critical users during periods of overload.

Add to Section C:
After contract award, the contractor shall deliver a draft continuity of operations plan for the system being acquired for agency approval within ninety days of receiving the agency approval and/or guidance on the preliminary plan. The final continuity of operations plan shall be delivered ninety days after receiving agency approval and/or guidance on the draft plan. The plan shall be periodically reviewed and updated annually by the Contractor to ensure the accuracy and timeliness of the contents. Recommended updates and revision based on this review shall be submitted to the agency for approval _____ working days prior to incorporation in the plan.

Summary:
- Preliminary plan submitted with proposal;
- Draft plan submitted _____ working days after agency comment on preliminary plan; and
- Final plan submitted _____ working days after agency comment on draft plan.

The continuity of operations plan shall detail the taking of appropriate and timely action to protect system assets from damage or misappropriation in the event of the threat of a disaster or emergency. The emphasis shall be on avoiding or mitigating the damage caused by such things as fire, flood, or terrorist activity (modify to include threats to the system). The plan shall, at a minimum:

- Include a risk assessment;
- Identify essential functions or critical processes, components, and the relationship of critical workload to variables such as time to recovery;
- Identify activities that can be temporarily suspended;
- Identify alternate procedures; and
- Identity action(s) to be taken to mitigate threats.

The continuity of operations plan shall detail the taking of appropriate and timely action to return assets to use after damage, destruction, alteration or misappropriation. The system recovery portion of the plan shall include at a minimum:

- The basic strategy for recovery;
- Specifications for restoration procedures by component and subsystem priority; and
- Specific responsibilities for emergency response.

The continuity of operations plan shall state how the plan shall be tested and how often the tests shall be done. Annual testing is required as a minimum and some tests should be done without advance notice.

As part of continuity of operations/contingency planning, consider how long the system can be down.

In the event the system or any component is rendered permanently inoperative,

the contractor shall deliver a replacement within _____ working days from the date of request.

In the event the system or any component is unavailable for use due to maintenance or repair or other reasons for a period of more than ____ hours (or days), or in the event that it is reasonably anticipated that maintenance will exceed ____ hours, the contractor shall make a loaner or replacement available within ____ hours (or days).

C. Control of Information/Data

Contractors may have to work with information or data that the agency has designated as nondisclosable. Clauses should be used to prevent the contractor from disclosing the information during the course of the contract and after it has terminated. It is important to work with the contracting officer to ensure that nondisclosure is adequately addressed for both situations.

Any (list type of or all) information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an authorized officer or employee of the contractor shall require written approval of the contracting officer (or contracting officer's technical representative/COTR).

Any (list type of) information shall be accounted for upon receipt and properly stored before, during and after processing. In addition, all related output shall be given the same level of protection as required for the source material.

If it is necessary to disclose (type of) information to perform under the contract, the contractor shall request written authorization from the contracting officer (or COTR) to make such necessary disclosure.

(1) Except as provided elsewhere in this contract, the contractor shall not disclose (type of information) except to the individual specified in this contract.

(2) Only those disclosures specifically authorized in writing by the contracting officer (or COTR) may be made, and only when it is clearly shown by the contractor that such disclosures are essential to successfully perform under this contract.

(3) Should the contractor or one of his/her employees make any unauthorized disclosure(s) of confidential information, the terms of the Default clause (FAR 52.249-8), incorporated herein by reference, may be invoked, and the contractor will be considered to be in breach of this contract.

If nondisclosable information is released to prospective offerors in order for them to prepare proposals, the following clause can be used during the release of information.

I hereby certify that I will not disclose (type of information) unless authorized in writing by the contracting officer (or COTR). I agree that, whether or not a contract is awarded to me, I will keep all information confidential.

The following item is to prevent nondisclosable information from leaving the agency's control through such means as being on a disk drive sent out for maintenance.

The contractor shall ensure that (list type of) information shall not be released outside the control of the agency (or specific agency office),

including release for maintenance or replacement purposes, without the written consent of the contracting officer or COTR.

D. Security Documentation

Security documentation provides instruction about the use of the system security, assurance that the security requirement has been understood, and supports a demonstration of meeting the requirement. The items below are divided into proposal and deliverable documentation. In general, documentation that shows that a requirement has been understood will be received as part of the proposal and will be used to evaluate the offeror. Instructional documentation will, in general, be received as a deliverable after contract award. Documentation, such as test documentation, that demonstrates that the contractor has successfully met the security requirement will normally be received as a deliverable after contract award.

Depending on the nature of what is being acquired, these types of documentation can be mixed. For instance, an approach, abstract, or outline of a Security Features User's Guide can be included in the proposal with the final version as a deliverable. In the proposal phase, the document would be used to evaluate the offeror's understanding of the security requirement and their ability to meet the requirement. As a deliverable, this would become instructional documentation. Be sure documentation requested with the proposal is used for evaluation of the offer and does not constitute having the offeror prepare deliverables before award.

Depending on what is being acquired, be sure to get system level documentation, not just component documentation. For any type of documentation at the system level, the contractor should describe the system security requirement and how it has been implemented. The operating system documentation plus the security system documentation plus application documentation does not equal system documentation. System security documentation includes interrelationships among applications and with the operating system and utilities in its environment. Component documentation will generally be off-the-shelf, whereas system documentation will generally be developed by the contractor.

It may be necessary to provide additional detailed specifications, including content and delivery schedule, to give offerors and evaluators enough information to prepare/review cost estimates and to make objective evaluations.

PROPOSAL DOCUMENTATION

Offeror's strategy for security. This should be commensurate with the size and complexity of the system. All systems acquisitions should request some form of offeror security strategy. In this strategy, the offeror should state how the product or service will meet the security needs of the government. Offerors of off-the-shelf products should match the features of the packages to government specifications and address assurance. For complex system development efforts, this could include a plan for incorporating and assuring security throughout the development. An example of a clause requesting such a plan follows.

The offeror shall provide a plan that describes its automated information security program. The plan shall address the security measures and program safeguards which will be provided to ensure that all information systems and resources acquired and utilized in the performance of the contract by contractor and subcontractor personnel:

(1) Operate effectively and accurately;
(2) Are protected from unauthorized alteration, disclosure, or misuse of information processed, stored, or transmitted;
(3) Can maintain the continuity of automated information support for agency missions, programs, and function;
(4) Incorporate management, general, and application controls sufficient to provide cost-effective assurance of the system's integrity and accuracy, and
(5) Have appropriate technical, personnel, administrative, environmental, and access safeguards.

This plan will be included in any resulting contract for contractor compliance.

Offeror's internal security policy and plan. Procurements that include contract services can ask for this type of assurance document. Depending on the scope of the acquisition, this may include copies of the offeror's applicable computer security, personnel security, and physical security policies.

DELIVERABLE DOCUMENTATION

Security Features User's Guide. A description of the protection mechanisms provided by the system, guidelines on their use, and how they interact with one another. If a system is being procured, be sure to get system level documentation, as well as product documentation.

System Administrator/Facility Manual. A manual addressed to the system administrator that presents cautions about functions and privileges that should be controlled when running the system or facility in a secure manner. The procedures for examining and maintaining security features requested (such as audit record structures) should also be requested. The manual should describe the operator and administrator functions related to security, to include changing the security characteristics of a user. It should provide guidelines on the consistent and effective use of the protection features of the system, how they interact, warning, and privileges that need to be controlled in order to operate the system or facility in a secure manner. If a system is being procured, be sure to get system level documentation, as well as product documentation.

Test documentation. A report that describes the test plan, test procedures that show how the security mechanisms were tested and results of the security mechanisms' functional testing.

Design documentation. A report that provides a description of the manufacturer's or developer's philosophy of protection and an explanation of how this philosophy is translated in the system. This report can be the post-contract award counterpart of the offeror's strategy for security; it describes how the strategy was implemented. This can also include an informal or formal description of a security policy model and an explanation of how the system enforces the security policy. For systems requiring very high security assurance, formal description languages and mathematical modeling may also be included.

Additional information on documentation for automated systems is available from the following FIPS PUBs:

FIPS 38	Guidelines for Documentation of Computer Programs and Automated Data Systems
FIPS 64	Guidelines for Documentation of Computer Programs and Automated Systems for the Initiation Phase

E. Legal Issues

The contracting officer and the legal department need to be consulted about legal issues. This section addresses some issues that the procurement initiator may want to discuss with agency procurement and legal staff.

It is possible for computer products to cause security violations even if the products are functioning correctly. These violations could be caused by the product containing malicious code (i.e., virus or trojan horse), making operating system calls that bypass system controls, or containing undocumented backdoors that bypass security. Many manufacturers include backdoors so they can assist customers.

The FAR contains general clauses which define the respective responsibilities and allocate risks among the parties to a government contract. However, additional clauses may be needed to fully address specific computer security requirements. Such clauses, for example, may address guarantees, warranties, or liquidated damages. The specific wording of such clauses may vary from one solicitation to another because they are a function of the particular need for data integrity, confidentiality or availability and the nature of the system being protected.

Agencies may wish to consider the use of warranties, liquidated damages, and other clauses establishing the contractor's computer security-related responsibilities in contracts. Such clauses, when properly crafted, will provide incentive to the contractor to assure that its products and services meet the security requirements of the contract. Such clauses, when poorly drafted or overly broad, can unnecessarily increase contract costs, limit competition, complicate contract administration and increase litigation risk. These clauses must be prepared in conjunction with existing FAR clauses.

Warranties provide a means to require the contractor to fix products after they have been accepted. A warranty is an agreement by the contractor that it will be liable for meeting the contract specifications for a stated period of time after acceptance. (See FAR 46.7 and 52.246-17 through -20.)

Liquidated damages provide a means for the contractor to compensate the government for losses that result from contract delays or other problems. The purpose of liquidated damages clauses and other clauses fixing contractor's performance responsibilities in the computer security area is to provide incentive for the contractor to make sure that the product only does what it is intended to do and nothing more. For example, the product should be free from malicious code. This is done by having the contractor pay for damages that result from poor security. Since the goal is to acquire secure systems, the extent of the liquidated damages clause (or other such clause) should be commensurate with the anticipated risks and damage to the government. A specific maximum dollar value can be placed on the damages or other means can be used to limit the contractor's liability.

Note: These are not penalties. If a security violation occurs, but does not result in any loss, the contractor is not responsible for any liability or liquidated damage.

The following are examples of integrity statements which may be modified to form a warranty, guarantee, or liquidated damage clause. The examples are not intended to be used together and should be modified for the operating

environment. There are no examples of customized enforcement clauses (the specific warranty, guarantee, or liquidated damage) because they must be developed with the contracting officer and legal counsel. FAR 52.246-17 through -20 contain FAR standard warranties.

1. The subject product performs in accordance with all specifications, certifications, and representations reflected in the documentation provided in Addendum 1 except as reflected below:

   _____
   _____
   _____
   _____

2. The installation instructions provided with the subject product if properly followed shall result in the creation and modification of only those objects listed below:

   _____
   _____
   _____
   _____

3. The subject product (hardware or software) shall not interact with any other component (hardware, software, or firmware) of the system onto which it is being installed to perform any function not described in the documentation listed below:

   _____
   _____
   _____
   _____

4. The instructions provided for removing the subject product from any system onto which it has been properly installed, shall, if properly followed, release back to the system every object used to store the subject product on the system.

5. Other than the exceptions listed below, the subject product contains no undocumented functions and no undocumented methods for gaining access to this software or to the computer system on which it is installed. This includes, but is not limited to, master access keys, back doors, or trapdoors.

   _____
   _____
   _____
   _____

6. The subject product does not interfere or bypass the system security software [insert name(s) of security software]. The program code only performs request validation checking and enforces the action that the system security software indicates should be taken. This processing is done for all users. Any exceptions are listed below.

   _____

_____
_____
_____

Government patents and ownership of developed software and systems are another important considerations that should be discussed with the contracting officer and legal staff.

F. Administration, End of Task, Closeout

One issue for contract closeout is the return or destruction of government data/information. Since information can be easily copied, the return of originals does not fully address the destruction of the information. This issue only needs to be addressed when the government is having information processed on a contractor facility or computer. Be sure that official agency records or information is not destroyed before a copy of the information has been received by the agency (if needed).

The contractor certifies that the data processed during the performance of this contract shall be purged from all data storage components of its computer facility, and no output will be retained by the contractor after such time as the contract is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any agency data remaining in any storage component will be safeguarded to prevent unauthorized disclosures. (Insert schedule.)

Government furnished equipment (GFE) including hardware and software should be returned in accordance with normal procedures. Special computer security considerations include the return of the GFE in usable condition. This is especially important if a system is going to continue operation under the government's or another contractor's control. The computer security can be transferred by having passwords reset by the government or by having the contractor turn in the passwords. The delineation of security responsibilities during transition should be addressed. No specific language is provided because of the diversity and individuality of systems.

Returned software shall be certified to be in its original form.

Another item to be considered is computer accounts on government-owned systems. Accounts no longer needed by the contractor should be terminated to protect government resources, i.e., computer time, and to prevent malicious activity by unauthorized users.

When an employee no longer requires access to the system (if the employee leaves the company or the contract), the contractor shall notify the COTR within _____ working days. At contract completion or termination, the contractor shall provide a status list of all users and note if any users still require access to the system to perform work under another contract. Any group accounts or other means of gaining access to the system shall be listed also. This includes maintenance accounts and security bypasses.

If a user is fired or leaves the contract or company under adverse conditions, the contractor shall notify the COTR before the employee is removed. If the removal is unplanned, the contractor shall notify the COTR immediately after dismissing the employee. This will allow the government to terminate his/her access.

When an employee leaves a contract and at contract closeout, it is important to dispose of computer files as well as accounts. Often only the person who created/used the files has sufficient knowledge to dispose of them. If the contractor will be handling official agency records, be sure disposition is made in accordance with agency records management instructions.

When an employee leaves the contract, the contractor project manager shall

ensure that all files are disposed of by transfer to another user, archive, destruction, etc. The contractor project manager shall report (or certify) disposition in (time frame such as in a monthly report or within _____ weeks of the employee leaving.)

For complex contracts that include the development, implementation, or operation of a computer facility or application, a security working group can be used effectively to help maintain computer security. The group can be composed of a combination of government and contractor personnel. Depending on the operational environment, the group can be used for:

- information exchange;
- configuration management;
- certification and accreditation issues;
- analyzing security requirements;
- identifying new threats and vulnerabilities;
- identifying changes to the system that impact security;
- recommending solutions to security problems as they occur; and
- making recommendations based on tradeoffs between security and other functional requirements.

The following examples define a security working group used to support an operational system.

The contractor shall provide (number and type of) personnel for a security control/review group. This group will address security problems, help provide for the maintenance of accreditation or certification under the control of (government person responsible for computer security of system), report security problems, and make security recommendations.

The contractor can be responsible for the administration and support of the group.

The contractor shall schedule meetings monthly (or other time frame), arrange for (or provide) a room, and take minutes. The minutes will be submitted to the COTR/GTR within one calendar week after the meeting. The meetings shall commence one month (or other time frame) after contract award and continue throughout the period of performance (or other ending time).

G. Computer Security Training and Awareness

An important goal of the Computer Security Act is to have all personnel involved in the management, use, and operation of federal systems trained in computer security awareness and accepted computer security practices. OMB Circular A-130, Appendix III, specifically requires that contractor personnel involved in the management, operation, programming, maintenance, or use of federal systems be aware of their security responsibilities and how to fulfill them.

The following can be used in the cases where the agency determines that NIST Special Publication 500-172 "Computer Security Training Guidelines" adequately addresses the security training requirement for the contractor. This can be tailored to include specific additional skills, training levels, or audience categories depending on the requirements of the agency. A time frame should be specified for when the contractor personnel must have received the training. The development of training certifications should be discussed with the contracting officer.

The contractor shall, at a minimum, certify that all contractor personnel involved in the management, use, and operation of (name of) system(s) who perform work under the subject effort shall have received training appropriate to their assignment as defined in NIST Special Publication 500-172 "Computer Security Training Guidelines."

Each individual (or category of contractor personnel) proposed for the effort shall be identified with appropriate audience category(s), as defined in NIST Special Publication 500-172, pages 3-4. The contractor shall certify each as having received computer security training appropriate to their categories, as denoted in the training matrix on page 6 of 500-172 and described in pages 8-27.

Additional/refresher training shall be performed _____ (time period). Certification of this training shall be provided to the contracting officer no later than _____ calendar days after the training has occurred.

The following are examples of tailoring the training specification.

In addition, all contractor personnel involved in the administration of the access control package shall have received training on the package equivalent to ____ hours of classroom instruction or _____ hours of job experience using the package.

The contractor system security personnel shall have received training in the operations of the system that includes a systemic overview, the security features, known vulnerabilities and threats, and security evaluation methodologies.

The following can be used when the acquisition agency has specific training minimums that are available to the prospective offerors. The second paragraph may be added as an Instruction to Offerors.

The contractor shall, at a minimum, certify that any personnel who perform work under the subject effort shall have received security awareness and skills training that is equivalent to that received by government personnel at (fill in location).

It is the responsibility of the prospective offeror to obtain the agency guidelines for this training prior to the submission of a proposal under this solicitation at (fill in address and point of contact). (Alternate: The agency guidelines can be included as an attachment to the RFP.)

H. Personnel Security

Requiring vetting, or personnel screening, of contractor or subcontractor employees as a condition for access to government resources is a recommended safeguard. The type of access can be physical or computer systems access. The level of vetting should be based on an assessment of risk, cost, benefit, and feasibility. Vetting includes a range of implementations from minimal checks to full background investigations. The extent of screening is dependent on the sensitivity of the system or data and the implementation of other administrative, technical, and physical safeguards.

Be sure to include in the contract:

- what types of investigations are required for what types of access;
- who will review the investigation to determine access privileges;
- who is paying for the investigations;
- whether the investigations must be reviewed before access is granted;
- when names and supporting information must be submitted;
- what other types of clearances (from other government agencies) can be substituted; and
- how investigations or results will be reported on or certified to the contracting officer.

Different vetting could also be required for different types or levels of access. There are many kinds of investigations. OPM Federal Personnel Manual Chapter 736 Subchapter 3 describes some investigations as they pertain to government investigations. The list below includes those and other forms of investigations:

- Review of the employment forms completed by the individual;
- Personal reference check;
- Credit check;
- Verification of employment for the last 2 years prior to current employment;
- Verification of education (high school or beyond) within the last 5 years that resulted in the awarding of a degree;
- Local police check in present county and state;
- National criminal check by private agency;
- National Agency Check (NAC);
- National Agency Check and Inquiries (NACI);
- Minimum Background Investigation (MBI);
- Limited Background Investigation (LBI);
- Background Investigation (BI); and
- Special Background Investigation (SBI) that includes verification of all previous places of employment and residence for a several year period (e.g., 15 years).

Access to the government's resources is a privilege and should be revoked if an individual becomes a threat to the system.

The government may remove access privileges for contractor personnel for unauthorized, negligent, or willful actions. These may include, but are not limited to:

- exploration of the system;
- introduction of malicious software;

- unauthorized modification or disclosure of the system or data; and
- failure to logoff.

There are other types of personnel security methods besides investigations such as employee statements regarding conflict of interest. Conflict of interest can include procurement integrity certifications, financial disclosure, or reports on outside activity. Be sure to specify what is required, when the form(s) must be completed and what access decision(s) are based on the form.

If the agency has a computer systems user agreement that states user computer security responsibilities (such as safeguarding passwords), it is appropriate to require contractor personnel sign the agreement before computer systems access is granted. The following clause can be modified to be more stringent (such as agency receipt of agreement before access in granted).

The contractor shall insure that all contractor personnel sign the user agreement (sample attached in Section J of RFP) prior to having access to agency systems.

Care must be taken when addressing the area of contractor personnel. The government cannot engage in personal services contracts unless specifically authorized by statute. Personal services contracts are those where the government has an employer-employee relationship with contractor staff. See Part 37 of the FAR "Service Contracting." Requiring contractor personnel to be vetted as a condition for employment under the contract suggests an employer-employee relationship. However, requiring vetting of contractors as a condition for access to government resources is different. It does not imply an employer-employee relationship since the government has a responsibility to retain control of its resources.

While the distinction above may seem minor, it can be essential during a contract. It is important that the distinction is understood to avoid personal services contracts while protecting government resources.

I. Physical Security

The following types of clauses can be used for contracts where work will be performed at the contractor location.

Physical security for computer systems helps prevent theft, tampering, and destruction.

The contractor shall provide physical security for (list components or systems) other than those in agency controlled space and for information being transmitted across (list networks). Physical security measures to be implemented include protecting the:

- site (e.g., access to computer room);
- hardware (e.g., communications processors, modems); and
- software and data.

The contractor shall identify (name of system or components) equipment that will be in nonagency controlled areas. Methods for physically protecting these systems shall be provided by the Contractor. The protection shall be against damage, unauthorized access, alteration, modification and destruction, whether by act of nature, accident, or intrusion.

Computer security should be considered as an issue for preaward site surveys. In general, computer security should be integrated into existing agency clauses for preaward site surveys instead of using this clause.

When it is determined that a preaward site survey is necessary in order to verify that the security of a facility is adequate, the contracting officer shall notify the offeror that such a survey will be necessary and coordinate with the offeror as necessary. No contract for services or supplies will be awarded until the survey is completed. The recommendations of the (office performing survey), as appropriate, will be a significant factor in the determination of responsibility.

J. Computer Security Features in Systems

Computer security features in systems refer to specific functions to be incorporated or bought with applications, operating systems, and hardware. How security features are incorporated is dependent on the function and environment of the system.

For many systems, a combination of features will be used, some of which are incorporated in the operating system and some in the application. For example, additional access controls at a finer level of granularity (record or field) and edit checks are commonly incorporated at the application level, while file access may still be performed by the operating system. Many other security architectures are possible. Whatever security architecture is selected, it is imperative that the security features work together in the system environment and that the documentation and testing address the coordinated approach.

This section addresses several controls that are normally associated with operating systems but can be provided by an application. Additional application-oriented controls are described in FIPS PUB 73 Guidelines for Security of Computer Applications.

The features described in this section are a combination of basic security controls and some advanced controls. The controls are described in functional specifications. Individual tailoring to specific environments will probably be required. If the intention of the procurement is to acquire off-the-shelf products, market surveys should be performed to determine what features are currently commercially available. Modifying security features of off-the-shelf products can be expensive. (Market surveys should be performed in accordance with agency policy.)

This section, like the other sections in this guidelines, is a list of possible features, procedures, and assurances. Additional information on the uses of these features can be obtained from agency security officials and NIST and other publications. NIST Publication List 91, which is periodically updated, catalogues the NIST computer security publications. Technical terms and concepts are explained in the glossary.

Note: The term "system" is used loosely to mean any collection of components, hardware, software, firmware, processes, etc. The use of a more specific term is recommended. Terms such as "the offeror's solution" for integration efforts, "the product" for a component buy, "application system," "operating system," or specific references to parts of the system architecture, i.e., "trusted computing base," are a few examples.

Note: The controls are consistent with those specified in DoD's 5200.28-STD. See NCSL Bulletin Guidance to Federal Agencies on the Use of Trusted Systems Technology.

J.1. Identification and Authentication Specifications

Identification and authentication are basic building blocks of security features in systems. For many systems, every user initiated activity within the computer system (e.g., accessing or printing a file, sending a message) should be attributable to a user of the system. The identification is

normally performed when the user logs on to the system, whether through an interactive terminal, or through some other mechanism (e.g., using a batch job, through a network connection). User authentication is normally performed by use of a password. However, there are many methods of authentication. To enforce accountability and access control, all users must identify and authenticate themselves to the system.

The system shall include a mechanism to require users to uniquely identify themselves to the system before beginning to perform any other actions that the system is expected to mediate. Furthermore, the system shall be able to maintain authentication data that includes information for verifying the identity of individual users (e.g., passwords). The system shall protect authentication data so that it cannot be accessed by any unauthorized user. The system shall be able to enforce individual accountability by providing the capability to uniquely identify each individual computer system user. The system shall also provide the capability of associating this identity with all auditable actions taken by that individual. The system shall be able to maintain information for determining the authorizations of individual users.

The type of user authentication mechanism may need to be specified. The most common type of authentication is passwords. NIST FIPS PUB 112 Standard on Password Usage is a mandatory standard. In addition, DoD CSC-STD-00-85 Password Management Guideline contains further information on passwords.

There are several other types of authentication mechanisms. User authentication can be based on three categories of information: something the user knows, such as a password; something the user possesses, such as a token; and some physical characteristic (biometric) of the user, such as a fingerprint. Authentication methods employing a token or biometric can provide a significantly higher level of security than passwords alone. These systems are referred to as advanced authentication technology. In addition, cryptography is often incorporated into advanced authentication systems especially in network applications. NIST will be providing guidance on advanced authentication.

J.2. Discretionary Access Control Specifications

Computer systems access control is the mechanism used to specify "who" (subjects) can do "what" to items controlled by the system or application (objects). The most common types of access are read, write, modify, execute, and delete. The access control is said to be discretionary when users on the system can pass access permissions to other users. This can be done directly or indirectly, such as copying a file to a public area on the system.

(Note: The term "access control" is also used to refer to physical controls. This section addresses the logical access provided by the computer system.)

The system shall use identification and authorization data to determine user access to information. The system shall be able to define and control access between subjects and objects in the computer system. The enforcement mechanism (e.g., self/group/ public controls, access control lists) shall allow users to specify and control sharing of those objects by other users, or defined groups of users, or by both, and shall provide controls to limit propagation of access rights. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of

including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

Commercial systems vary significantly with respect to the granularity of objects to which discretionary access control is applied. Generally, operating systems are organized to provide discretionary access control at the file level. In order to provide access control within an application, the government must specify the types of objects, such as data elements, that are subject to the access control.

If system being acquired is to be delivered with access controls established, then the government must provide a security policy, definition of data objects, and list of access classes, access types, and accesses (who can do what) to the data objects.

J.3. Audit Specifications

Auditing provides protection in the sense that all meaningful actions within the system may be recorded and some user held accountable for each action. Auditing can occur at the operating system level or within a database or application. The recorded audit data can assist the system security officer in determining who is responsible for a problem or how a problem was caused. Audit data can be used to deter users from attempting to exceed their authorizations and to achieve individual accountability. The key to accountability in computer and network systems is the recording and analysis of effective audit trail information.

Some system designers provide for the auditing of an event with mechanisms that cannot be turned off by the operator, or system security officer. Other system designers supply audit capabilities that can be turned on or off at the discretion of the operator or security officer, thus allowing each local site to "tune" its auditing. There are a number of tradeoffs that must be made in deciding what is to be audited and how often.

The government is responsible for selecting which events have the potential to be audited and, after system acquisition, which events are recorded in the audit trail. The government must also specify how long audit information is to be retained and on what media. These decisions should be based on how the audit data will be used.

The following is a three-part specification for auditing which should be modified for the type of system being procured. The first part of the specification defines the auditing function itself.

The system shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected so that read access to it is limited to those who are authorized.

The second part of this specification lists what types of events need to be auditable. This list should be modified to include security events relevant to the system function and environment.

The system shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a

user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators and/or system security officers and other security relevant events. The system shall also be able to audit any override of human-readable output markings.

The third part of this audit specification is a description of the audit record.

For each recorded event, the audit record shall be able to identify: date and time of the event, user, type of event, and success or failure of the event. For identification/ authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events, the audit record shall include the name of the object and the object's label. The system administrator shall be able to selectively audit the actions of any one or more users based on individual identity and/or object label.

J.4. Cryptography Specifications

The following subsections address some of the ways cryptography can be used to provide computer security services in systems and some of the considerations for using cryptography.

Cryptography can be used to provide confidentiality and integrity protection and can be used in the generation of electronic signatures. Confidentiality of information can be provided through encryption, which is the process of transforming information from a human intelligible form to an unintelligible form. Integrity can be provided through message authentication, which is a cryptographic process used to detect unauthorized changes to information (transmitted or stored) in a computer system. An electronic (cryptographic) signature is used as a replacement for a handwritten signature.

Cryptography can be categorized as either secret key or public key. Secret key cryptography is based on the use of a single cryptographic key shared between two parties. The same key is used to encrypt and decrypt the data. Public key cryptography uses two keys: a private key which is known only to its owner and a public key which is distributed. Either the public or private key can be used to encrypt the data and the opposite key is used to decrypt it.

Choosing which type of cryptography should be implemented in a system is determined by several factors. An agency should consider the requirements of the application and the types of services which can be provided by each type of cryptography. It is possible that both secret key and public key cryptography are needed in one system; each performing different functions.

This section addresses three services provided by cryptography; encryption, data authentication, and electronic signatures; and two areas that must be considered for any system using cryptography: key management and security of cryptographic modules.

J.4.a. Encryption

If encryption of sensitive but unclassified information (except Warner

Amendment information) is needed in a federal information processing system the use of the Data Encryption Standard (DES), FIPS 46-1, is required unless a waiver is granted by the head of the federal agency. The NCSL Bulletin on DES dated June 1990 provides an overview of DES, addresses its applicability, and describes waiver procedures. Procurement initiators should be aware that software implementations of the algorithm for operational use in general purpose computer systems currently do not comply with the standard, and, if used, a waiver is required.

NIST provides a validation service for DES. A validation is required for conformance with the standard. See section 4.f below and Appendix B for further information on validations and assurances, including contract language.

The encryption provided by (the system or specific part of the system as defined in the statement of work) shall be accomplished in accordance with FIPS 46-1 Data Encryption Standard. (Select validation language from Appendix B.)

In addition to specifying the cryptographic implementation, agencies should consider other technical variables such as throughput, system interfaces, and data format. While DES can work in any environment, the product that implements the DES may have been customized for a particular environment.

Other important aspects of DES, such as key management and the security of the modules, are addressed in sections 4.d and 4.e.

J.4.b. Data Authentication

DES is the basis for the Data Authentication Algorithm defined in FIPS 113, Computer Data Authentication. The FIPS 113 provides integrity for information using a cryptographic check value known as the Message Authentication Code (MAC). Applying the DES algorithm, a MAC is calculated on and appended to information. To verify that the information has not been modified at some later time, the MAC is recalculated on the information. The new MAC is compared with the MAC that was previously generated and if they are equal then the information has not been altered. This standard should be used by agencies whenever cryptographic authentication is needed for the detection of intentional modification of information.

Note: FIPS 113 may be implemented in hardware, software, firmware, or any combination thereof.

NIST provides a validation service for FIPS 113. Agencies may require that offerors have products tested. For many applications, validation testing can provide cost-effective assurance. See section 4.f below and Appendix B for further information on validations and contract language.

The data/message authentication provided by (the system or specific part of the system as defined in the statement of work) shall be accomplished using message authentication codes as defined by FIPS 113. (Select validation language from Appendix B.)

J.4.c. Electronic Signature

Using cryptography, an electronic signature capability has been developed as a replacement of the handwritten signature. This capability can be used in ADP systems anywhere a signature is required. For example, a signature may be needed on an electronic letter, form, or message. Like the handwritten signature, the electronic signature can be used to identify the originator or signer of ADP information. Unlike its written counterpart, it also verifies that information has not been altered after it was electronically signed.

An electronic signature can be generated using public key or secret key cryptography. Using a public key system, documents in a computer system are electronically signed by applying the originator's private key to the document. The resulting digital signature and document are usually stored or transmitted together. The signature can be verified using the public key of the signer. If the signature verifies properly, the receiver has confidence that the document was signed by the owner of the public key and that the message has not been altered after it was signed. Because private keys are known only to their owner, it is also possible to verify the signer of the information to any third party. A digital signature, therefore, provides two distinct security services: nonrepudiation and message integrity. Identifying that electronic information was actually signed by the claimed originator to a third party provides nonrepudiation. Determining that information was not altered after it was signed provides message integrity. NIST currently has a draft Digital Signature Standard (DSS), which has not yet been assigned a FIPS number.

NIST is planning on providing a validation service for the DSS. A validation will be required for conformance with the standard after NIST establishes the validation program. See section 4.f below and Appendix B for further information on validations and assurances, including contract language.

The following contract clause should not be used until the draft FIPS is finalized.

The public key-based digital signature capability provided by (the system or specific part of the system as defined in the statement of work) shall be accomplished in accordance with the Digital Signature Standard (insert FIPS number). (Select validation language from Appendix B.)

Using DES, a secret key algorithm, a MAC (a cryptographic check value) can be used to provide an electronic signature capability. Calculating a MAC on information in an ADP system provides message integrity as described in section 4.b above. A MAC can be used to identify the signer of information to the receiver. However, the implementations of this technology do not inherently provide nonrepudiation because both the sender of the information and the receiver of information share the same key.

The electronic signature capability provided by (the system or specific part of the system as defined in the statement of work) shall be accomplished in accordance with FIPS 113. (Select validation language from Appendix B.)

J.4.d. Key Management

Key management is extremely important because the security of any cryptographic system is dependent on the security provided to the cryptographic keys. In order for a cryptographic system to work effectively, keys must be generated, distributed, used, and destroyed securely. Key

management is an issue in both secret key systems, such as DES, and public key systems. This section addresses secret key systems.

NIST has developed a draft FIPS PUB for the management of cryptographic keying material utilizing the Data Encryption Standard. (A FIPS number has not yet been assigned.) The draft FIPS PUB adopts ANSI X9.17 and specifies a particular selection of options for the automated distribution of keying material by the Federal Government. This standard must be used by Federal agencies when designing, acquiring, implementing and managing keying material which use DES and ANSI X9.17. Other key management systems may be approved by NIST for federal government use in the future.

NIST provides a validation service for selected options of ANSI X9.17 and is developing services for the new FIPS. Agencies may require that offerors have products tested. For many applications, validation testing can provide cost-effective assurance. See section 4.f below and Appendix B for further information on validations and assurances, including contract language.

The following contract clause should not be used until the draft FIPS is finalized. Make sure that the validation section of the clause only specifies options for which NIST is currently providing validation services.

The key management provided by (the system or specific part of the system as defined in the statement of work) shall be accomplished in accordance with (insert FIPS number).

Key management can be a complex issue for large or diverse systems. Be sure to request a key management system that meets the system's specific needs.

J.4.e. Security of Cryptographic Modules

The security of cryptographic modules refers to the secure design, implementation and use of a cryptographic module. The security of cryptographic modules is important because cryptography is often relied on as the exclusive means of protecting data when the data is outside the control of the system. The protection of the data is, therefore, reliant on the correct operation of the cryptographic module. The knowledge that a module is operating correctly is referred to as assurance. Appendix B and section III.B.1.b further discuss assurance.

Proposed FIPS PUB 140-1 Security Requirements for Cryptographic Standards establishes the physical and logical security requirements for the design and manufacture of cryptographic modules used to protect sensitive unclassified information. Note: FIPS 140-1 can be used to provide assurance for DES and other NIST-approved cryptographic algorithms, such as the public key algorithm used in the digital signature standard.

FIPS 140-1 defines four levels of security, with Level 1 being the lowest and Level 4 being the highest. Based on the level of assurance analysis performed during the security requirements phase (sec. III.B.1.b), an appropriate FIPS 140-1 level should be identified. NIST may provide additional information which will help agencies identify the appropriate level. The identification of the security level should be specified in the procurement package.

FIPS 140-1 will replace FIPS 140, General Security Requirements for Equipment Using the Data Encryption Standard (formerly Federal Standard 1027).

Currently agencies must require conformance with FIPS 140 (or obtain a waiver) if cryptography is used to protect sensitive unclassified information. Since testing is no longer available for FIPS 140, agencies cannot require validation testing. Instead, agencies should require an offeror's declaration of FIPS 140 conformance or, if available, an NSA endorsement. After FIPS 140-1 becomes a standard, agencies should continue to require a declaration of conformance until NIST establishes the validation service. Only then can agencies require FIPS 140-1 validations. The CSL Bulletin, "FIPS 140 - A Standard In Transition," dated April 1991, provides additional information on the standard and the waiver procedure.

When FIPS 140-1 becomes a standard and NIST has established the validation program, the following clause can be used. A validation will be required for conformance with the standard. See section 4.f below and Appendix B for further information on validations and assurances, including contract language. These clauses should not be used until FIPS 140-1 is finalized.

The design, implementation, and use of the cryptographic module provided by (the system or specific part of the system as defined in the statement of work) shall be in conformance with FIPS 140-1, Level (insert level). (Select validation language from Appendix B.)

J.4.f. Validations

NIST currently provides validation services for FIPS 46-1, FIPS 113, and selected options of ANSI X9.17. After an implementation is validated, NIST issues a validation certificate and adds the implementation to a Validation List. (Lists for validated implementations are available by contacting NIST or through their electronic bulletin board service, 301-948-5717 or from the NIST Validated Products List, updated quarterly.) Manufacturers, integrators, and offerors may purchase validated implementations and use them in their own products. As long as the validated implementation has not been altered, a second validation is not performed. Therefore, the product containing the validated implementation would not be on the validation list; however, the offeror should be able to identify the validated implementation used in the product or supply a copy of the original validation certificate.

See Appendix B for more information on validations and assurance. Appendix B specifically addresses options for validation testing and provides contract language.

Other Sources

NIST has other standards and guidelines that relate to cryptography. A list of NIST publications is available from NIST Publications List 91. For ordering information, see the inside back cover of this document.

J.5. Object Reuse Specifications

When a system resource (memory or storage) is reused, there is a possibility that the new user can view "residual information" left in the resource by the previous user. The purpose of object reuse specifications is to prevent the inadvertent disclosure of residual information. Since object reuse may impact system performance, care should be taken in selecting and testing object

reuse.

The system shall be able to ensure that all authorizations to the information contained within an object are revoked prior to initial assignment, allocation or reallocation to a subject from the system's pool of unused objects. The system shall be able to ensure that no information, including encrypted representations of information, produced by a prior subject's actions is available to any subject that obtains access to an object that has been released back to the system.

Object reuse specifications can be achieved either by clearing objects upon allocation or upon deallocation. A third method involves establishing a "high water mark" sensitivity of the object, allocating it only to processes of the same sensitivity. Objects can be cleared by overwriting each bit in the object. The minimum number of overwrites should be specified.

J.6. System Integrity Specifications

The government can use commercial off-the-shelf diagnostic capability for validating correctness of the hardware and firmware operations. Generally speaking such diagnostic offerings are not valid to verify the correctness of the software implementation.

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the system.

In addition, some vendors are using cryptographic techniques to verify the integrity of their software. These can be used to ensure that software received, or in storage, is the same as the "master" copy of the software maintained by the vendor.

J.7. System Architecture Specifications

As described in Appendix B, "Assurance," the use of advanced system architectures can provide assurance that the security features are correctly and effectively implemented.

The mechanisms within the application that enforce the access control shall be continuously protected against tampering and/or unauthorized changes.

The security-relevant software shall maintain a domain for its own execution that protects its security mechanisms from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the system may be a defined subset of the subjects and objects in the computer system. The system shall maintain process isolation through the provision of distinct address spaces under its control. The system shall isolate the resources to be protected so they are controlled by the access control and auditing requirements.

Note: The word "domain" as used here refers to the protection environment in which a process is executing. Domain is sometimes also referred to as "context" or "address space."

The procuring agency should be aware that over specification of the

architecture for a system can preclude integrators from incorporating otherwise valid existing products. Over specification can also eliminate lower cost alternatives resulting in a more costly procurement. This over specification is a common problem and generally proves not to be cost effective. From a security perspective over specification can actually preclude adequate information control.

J.8. Labels and Mandatory Access Control

The following sections address labels and mandatory access control. These are emerging security features in some off-the-shelf operating systems which may be appropriate for use in some computing environments. They are not required.

This section presents a brief introduction to and specification language for labels and mandatory access control. Labels and mandatory access control should not be acquired or implemented without a thorough knowledge of access control policy, information flow, and how labels and mandatory access control work. Labels and mandatory access control can be costly in terms of dollars, ease of use, ease of administration, and computer resources.

These sections on labels and mandatory access control are addressing only one form of mandatory access. Other approaches, such as those based on roles, are possible. section J.9 addresses labels; section J.10 addresses mandatory access controls. For additional guidance, the procurement initiator should contact the agency security official.

Labels and mandatory access control are useful when acquiring multi-user computer systems with a requirement for mandatory separation of sensitive information and for which security labels can be established. In practical terms, this means labels and mandatory access control are most useful if the type and degree of sensitivity of the data can be established, and there is a strong reason for using technical means to enforce compliance with policy. Labeling and mandatory access control require that there is a clear access control policy that can be enforced.

J.9. Label Specifications

Labels can be used to have the system manage sensitive objects. A label is a piece of information that represents information about an object or subject. Labels can be used for a variety of purposes including access control, specifying protective measures, and indicating additional handling instructions. This document addresses using labels for access control. It should be modified if the labels will be used for other purposes. If labels are used for access control, then object labels represent the degree and type of sensitivity of the data in an object. Subject labels represent the authorization of users to access degrees and types of sensitive data.

Security labels associated with each subject and storage object under the system's control (e.g., process, file, segment, device) shall be maintained by the system. These labels shall be used as the basis for access control decisions. In order to import nonlabeled data, the system shall be able to request and receive from an authorized user (e.g., system or application security administrator) the security label of the data, and all such actions shall be auditable by the system.

In order to ensure smooth transition in the operating conditions of the system when changes are necessary, and also for maintenance purposes, it is sometimes necessary to provide capabilities that allow the security labels of objects to be altered under carefully controlled conditions.

The system shall ensure that any feature that changes security labels is only invocable by an authorized individual under the direct control of the system, or by a part of the system, and that these actions are subject to auditing requirements.

J.9.a. Label Integrity Specifications

The following specification addresses integrity requirements for labels. Depending on system architecture, it is not essential that a label be maintained with the data. It is permissible to associate the label with the data. Some operating systems maintain the label inside the operating system and store the data separately.

Security labels shall accurately represent the degree and type of sensitivity of the specific subjects or objects with which they are associated. Throughout the system, security labels shall accurately and unambiguously represent and be associated with the information being managed.

J.9.b. Labels and Input/Output Specifications

Since all systems receive input (import data) and produce output (export data), the system designer must address the problem of what to do with labels at system boundaries. How is incoming data labeled? How is outgoing data labeled? The input and output can be in electronic, paper, or other form.

The system shall be able to designate each communication channel and I/O device as either single-label or multi-label. Any change in this designation shall be done by a properly authorized individual and shall be auditable by the system. The system shall maintain and be able to audit any change in the security label or labels associated with a communication channel or I/O device.

The Phrase "Properly Authorized" is understood to be the System Administrator and Security Officer or their designees.

J.9.b(1) Multi-Label Communications

When information contained in an object is exported from the system, a means must be provided for the system to accurately and unambiguously associate the security label of the object with the information being exported. The Phrase "exported by the system" is understood to include transmission of information from an object in one system to an object in another system. The form of internal security labels may differ from their external (exported) form, but the meaning must be retained. This association is critical on multi-label channels because the receiver will use the provided label both for processing and access decisions.

When the system exports an object to a multi-label I/O device, the security label associated with that object shall also be exported and shall reside on

the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When the system exports or imports an object over a multi-label communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the security labels and the associated information that is sent or received.

J.9.b(2) Single-Label Communications

Two types of single label designations are possible. One type can be applied to a channel or device by a Security Administrator. The second type can be applied by an authorized user (e.g., application security administrator) who can designate which label, within a range, is to be applied to the subsequent data/object. Thus a device or channel may be multiple consecutive single labels; but the system must communicate with an authorized user prior to each label designation change.

Single-label I/O devices and single-label communication channels are not required to maintain the security labels of the information they process. However, the system shall include a mechanism by which the system and an authorized user (e.g., application security administrator) reliably communicate to designate the single security label of information imported or exported via single-label communication channels or I/O devices.

J.9.b(3) Labeling Output

The following specifications address exporting data to a different environment, for example, from the internal system environment to the office environment or a networked environment.

Prior to releasing an object to an environment where accesses are no longer mediated by the system, the system must associate the object with an external label that is comprehensible to the new environment. The external label must accurately represent the security label of the object as assigned by the system.

One of the most common examples of moving a label into a new environment is labeling human-readable output, specifically printouts. The following specification is an example of how the system can label printouts.

The system administrator shall be able to specify the printable label names associated with exported security labels. The system shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable security labels that properly represent the overall sensitivity of the output. The system shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable security labels that properly represent the overall sensitivity of the output or that properly represent the sensitivity of the information on the page. The system shall, by default and in an appropriate manner, mark other forms of human-readable output (e.g., maps, graphics) with human-readable security labels that properly represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the system.

The system administrator is usually the "user" designated to specify the printed or displayed security label that is to be associated with exported

information.

J.10. Mandatory Access Control Specifications

As stated in section 2, access control is the mechanism used to specify "who" can do "what" to items controlled by the system. The most common types of access are read, write, modify, execute, and delete. The access control is said to be mandatory when the system mediates access based on subject and object labels. This prevents users from accidentally or deliberately violating the access control policy.

The system shall be able to enforce a mandatory access control policy over all subjects and storage objects (e.g., processes, files, segments, devices). These subjects and objects shall be assigned security labels and shall be used as the basis for mandatory access control decisions. The system shall be able to support two or more such labels. The following requirements shall hold for all accesses between subjects and objects controlled by the system:

- A subject can read an object only if the hierarchical attribute in the subject's label is greater than or equal to the hierarchical attribute in the object's label and the nonhierarchical attribute in the subject's label include all the nonhierarchical attributes in the object's label.

- A subject can write an object only if the hierarchical attribute in the subject's label is less than or equal to the hierarchical attribute in the object's label and all the nonhierarchical attributes in the subject's label are included in the nonhierarchical labels in the object's label.

- Identification shall be used by the system to ensure that the authorization of subjects created to act on behalf of the individual user are a subset of the authorization of that user.

Appendix A

Uniform Contract Format for Federal Government
Requests For Proposals (RFP)

RFP Section	Contents	Created By Technical and/or Procurement Comments
A. Solicitation/Contract Form	Cover Sheet For RFP, with Solicitation Number, Type of Solicitation, Due Date, Procurement Contact Point, etc. (SF33)	Procurement Contains standard RFP information
B. Supplies or Services and Prices/Costs	List of Products/Services to Be Provided by Offeror	Procurement Developed from other portions of RFP. Contains standard RFP information.
C. Description/ Specifications/ Work Statement	Defines Scope of Contract and Requirements Including: Mandatory Specifications, Optional Features Services Specification may be included as an Attachment/Section J	Technical & Procurement Describes product/services to be procured.
D. Packaging and Marking	Shipping, Handling, and Storage Requirements. May Not Be Required For Service Contracts.	Procurement & Technical Standard RFP information with special technical requirements if necessary.
E. Inspection and Acceptance	Standards of Performance, Reliability Requirements, Acceptance, Benchmarks, Inspection, Quality Assurance	Procurement & Technical Determines how product or service is to be accepted and must perform. Contains standard RFP information with specific technical requirements.
F. Deliveries or Performance	Time, Place, and Method of Deliverables/Performance. Describes such things as:	Procurement & Technical Contains standard

		Liquidated Damages, Equipment Replacement, Field Modifications, Alternations, Maintenance Response Time and Down Time Credits, Product Replacement, Variation in Quantity, Delivery and Installation Schedule, Stop Work Orders, Etc.	RFP information with special technical requirements.
G.	Contract Administration Data	Contract Administration such as: Authorities of Government Personnel, Required Reports, Holidays, Use of Government Property, Financial Information	Procurement & usually Technical Normally standard RFP information with special technical requirements.
H.	Special Contract Requirements	Clauses Other Than Those Required By Law/Regulations Including: Warranties, Replacement Parts, Engineering Changes Recording Devices, Hardware/Software Monitors, Site Preparation, Financial Reporting, Transition Requirements, Handling of Data, Security, Etc.	Procurement & Technical Normally standard RFP information with special technical requirements.
I.	Contract Clauses	Clauses Required By Law/ Regulations not Otherwise Required for a Particular Section.	Procurement Contains standard RFP information
J.	List of Attachments	Any Additional Procurement and Technical Information For Offeror.	Procurement & Technical
K.	Representations, Certifications, and Other Statements of Offerors	All Statements Required of the Offeror by Law/ Regulation/Agency. Offeror Must Complete and Return with proposal.	Procurement Standard RFP information
L.	Instructions, Conditions, and Notices to Offerors	Requirements for Proposals. Specifies the Plans, Approaches, References, and Other Information the Offeror Must Submit Proposal Evaluation. Requires Offeror To Tell	Procurement & Technical Addresses how offeror should respond to statement of work as set out in the evaluation criteria.

	How They Will/Can Meet The Requirements Described In Section C.	
M. Evaluation Factors For Award	Describes How Proposals Will Be Evaluated and the criteria against which proposal will be evaluated. Also Describes how a Source will be selected.	Procurement & Technical

For further information, see FAR 15.406.

Appendix B

Assurance

There are many methods of attaining assurance that the security features work as proposed. Since assurance methods tend to be qualitative rather than quantitative, they will need to be evaluated. Assurance can also be quite expensive, especially if extensive testing is done. It is useful to evaluate the amount of assurance received against the cost to make a best value decision. It is important to consider assurance methods within the context of the statement of work, evaluation plan, and acceptance test plan.

The selection of assurance methods should be consistent with and follow from the requirements analysis, especially from the risk analysis. Since some of the methods are impossible for certain types of federal information processing (FIP) acquisition or are restrictive of competition, care must be taken in selection. See the note on assurance and competition at the end of this appendix.

It will normally be best to use a combination of methods. Each method has strengths and weaknesses in terms of cost and what kind of assurance is actually being delivered. None are foolproof. Each method has restrictions. An accrediting and/or certifying official or computer security official can help determine the strengths and weaknesses of each method based on the type of system(s) being procured.

Many of these assurances are evaluations. Care must be taken to know what evaluation criteria were used and exactly what the evaluation means. Evaluations and testing all have limits. No organization can afford to test every possibility including how the evaluated item interacts with other system components.

Methods

Testing/quality assurance. There are many techniques that have been developed for use with "critical" or high assurance systems. These techniques can be applied to security software. These development and acceptance techniques provide assurance for systems. The following NIST publications provide further explanation:

FIPS PUB 101	Guideline for Lifecycle Validation, Verification, and Testing of Computer Software
FIPS PUB 132	Guideline for Software Verification and Validation Plans
SP 500-144	Guidance on Software Package Selection
SP 500-165	Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Product Management Standards
SP 500-180	Guide to Software Acceptance

Agency quality assurance, safety, or reliability personnel may also be able to provide assistance. The contractor developing the system or application can provide security testing. The development and acceptance testing can also be done by an independent validation and verification contractor (IV&V). If testing is going to be done by an independent contractor, this needs to be specified in the RFP.

NIST conformance testing and validation suites. NIST produces validation suites and conformance testing to determine if a product (software, hardware, firmware) meets specified standards. These test suites are developed for specific projects and use many methods. New test suites are being developed. In general, testing is performed by the vendor and validated by NIST, or testing is performed by a certified laboratory. Following are examples of two types of NIST computer security testing:

- DES implementation testing (reference Special Publication 500-20). To validate the correctness of the implementation, vendors run specified tests and send the results to NIST. If the vendor passes the test, NIST issues a validation certificate.

- FIPS PUB 113 data authentication algorithm testing and ANSI X9.17 key management for point-to-point environments. Vendors connect to a NIST bulletin board that interactively runs the test suite for the selected standard. If the vendor passes the test, NIST issues a validation certificate.

Evaluations by government agencies. Government agencies evaluate products for use in their environments. These evaluations may or may not be published. It is important to ask offerors to supply evaluation results as part of an assurance package. These evaluations are normally not endorsements by the agencies.

NSA's Evaluated Products List (EPL). The National Security Agency (NSA) evaluates some computer operating systems and security packages against DoD 5200.28-STD, Trusted Computer Systems Evaluation Criteria (TCSEC or Orange Book).

Evaluations by independent organizations. Trade and professional organizations are possible sources of independent evaluations. Ask offerors to provide information on evaluations which they consider pertinent to their proposal.

Evaluations by another vendor. Private commercial organizations may offer product assurance testing and evaluations. These may lack the independence of government and trade organization evaluations.

Evaluations by another government. Other governments, including several European governments and Canada, are researching evaluation techniques and criteria. Care should be taken to observe the differences in environments and governmental priorities.

Product has been accredited to operate in similar situation. Once again, these accreditations are not published. It is important to ask offerors to supply the accreditation results. These, even more so than evaluations, are not normally endorsements. Accreditations are environment and system specific. Since accreditation balance risk against advantages, the same product may be accredited for one environment but not for another.

Self-certification following a formal procedure, e.g., FIPS 102. A vendor self-certification does not rely on the work of an impartial or independent reviewer. It is a vendor's technical evaluation of a system to see how well it meets an internally stated security requirement. Even though this method does not provide an impartial review, it can still provide some assurance.

The vendor's reputation is put on the line and a certification report can be read to determine if the security requirement was defined and if a meaningful review was performed.

Self-certification under the auspices/review of an independent organization. This method may be able to combine the lower cost and greater speed of a self-certification with the impartiality of an independent review. The review, however, may not be as thorough as an evaluation or testing.

Warranties, Integrity Statements and Liabilities. Warranties are another source of assurance. If a manufacturer/producer is willing to correct errors within certain time frames or by the next release, this should give the purchaser a sense of commitment to the product and of product quality. An integrity statement is a formal declaration or certification of the product. It can be backed up by a promise to (a) fix the item (warranty) or (b) pay for losses (liability) if the product does not conform to the integrity statement. See section IV.E, "Legal Issues," for more information.

Manufacturer's published assertions. A manufacturer's or developer's published assertion or formal declaration provides assurance based on their reputation.

Assurance documentation. There are several types of assurance documentation. Descriptions are provided in section IV.D, "Documentation."

Use of advanced or trusted development. Offerors may provide documentation to show that they have used advanced or trusted system architectures, development methodologies, or software engineering techniques. Use of the trusted computing base (TCB) concept, formal modeling, and mathematical proofs are some examples. Offerors should describe how these techniques and methodologies were employed and how they help protect the system. (A specification for a trusted computer base architecture is included in "Features in Systems," sec. IV.J.7.)

Assurance Methods and Competition.

Since not all assurance methods are equally available to all vendors, requiring any one assurance method can limit competition. This is especially true for evaluations. If the government specifies that a product pass a certain test to get on a list of "qualified" products before it is acquired, then there may be special rules that must be followed. FAR 9.2 addresses qualified products.

The government, according to a basic procurement philosophy, tries to maintain a "level playing field" while providing incentive for vendors to provide advanced products. Requiring that a vendor use an assurance method that is not accessible by all vendors limits competition and may preclude the government from considering new ideas.

There are many methods for increasing competition while still meeting the government's requirements. Discuss with the contracting officer the use of scoring assurance methods or providing incentives and disincentives. These can be used to "give credit" to offerors who have had their products evaluated while maintaining full and open competition.

Note: In a scoring scheme, it must be possible for an offeror to gain the maximum number of points possible using assurance methods that are equally

accessible to all.

Contract Language for Validation Testing

The following considerations and contract language, based on the Federal ADP & Telecommunications Standards Index, can be used to help increase assurance and promote competition. Although the clauses are addressed to the use of NIST conformance and validation testing, they can be modified for use with other forms of assurance. (Note: Some NIST validations, such as DES validations, are required and some are optional.)

Testing and validations can be performed at several stages during an acquisition. These clauses address three types of testing: delayed validation, prior validation testing, and prior validation. For delayed validation and prior validation testing, be sure to customize the time frame parameter in Part 2 of the solicitation wording to ensure that any resubmissions for validations are done in a timely manner.

Delayed Validation. When an agency determines that the nature of the requirement is such that implementations of a FIPS may be offered that have not yet been tested for conformance to that FIPS or if an implementation of the FIPS will be developed during the course of the contract, the "Delayed Validation" solicitation wording option should be used.

Prior Validation Testing. When an agency determines that it is essential for implementation of a FIPS to be previously tested for conformance to that FIPS before being offered, and the nature of the requirement is such that an implementation of a FIPS may be initially offered that has not been fully validated (i.e., implementation has not fully demonstrated compliance to the FIPS), the "Prior Validation Testing" solicitation wording option should be used. For example, some validation procedures, especially for complex FIPS, allow for stages within the process.

Prior Validation. When an agency determines that it is essential for implementations of a FIPS be validated (i.e., implementation has been tested and has demonstrated compliance to the FIPS) for conformance to that FIPS prior to being offered the "Prior Validation" solicitation wording option should be used.

Solicitation Wording: Validation of FIPS Implementations

This clause can be modified to address particular FIPS and particular system components. Within a solicitation, different testing options can be specified for different components.

In addition to the FIPS implementation requirements specified elsewhere in this requirements document, all implementations of FIPS that are brought into the Federal inventory as a result of this document for which validation is specified, and those implementation used by vendors to develop programs or provide services shall be validated using the official validation system specified by the National Institute of Standards and Technology (NIST) Computer Systems Laboratory (CSL). Validation shall be in accordance with CSL validation procedures for that FIPS. The results of validation shall be used to confirm that the implementation meets the requirements of the applicable FIPS as specified in this document.

To be considered responsive the offeror shall:

(1) Provide validated FIPS implementation through (select testing option and insert appropriate paragraph from below: "Delayed Validation," "Prior Validation Testing" or "Prior Validation.")

(2) Agree to correct all implementation nonconformance from the applicable FIPS reflected in the validation summary report not previously covered by a waiver. All areas of nonconformance must be corrected within 12 months (or other time frame) from the date of contract award (or from the date of the summary report) unless otherwise specified in this document. If an interpretation of the FIPS is required that will invoke the procedures set forth in FIPS PUB 29-2, such a request for interpretation shall be made within 30 calendar days after contract award. Any corrections that are required as a result of decision made under the procedures of FIPS PUB 29-2 shall be completed within 12 months of the date of the formal notification to the contractor of the approval of the interpretation. Proof of correction in either case shall be in the form of a CSL Certificate of Validation or registered validation summary report for the corrected implementation. Failure to make required corrections within the time limits set forth above shall be deemed a failure to deliver required material. The liquidated damages as specified for failure to deliver the operating system or other system component (software, hardware or firmware) shall apply.

Testing Options:

"Delayed Validation"

> The offeror shall certify in the offer that all implementation of FIPS, including applicable FIPS options, offered or developed in response to this document will be submitted for validation. If the implementations are to be developed they shall be submitted for validation upon delivery. If the implementations are available and have not been previously tested or validated then the implementations shall be submitted for validation upon contract award. In either case, when the implementation is submitted for validation the submission shall include a request to have the validation be completed at the earliest possible date permitted by the CSL validation procedures. Unless specified elsewhere, proof of submission for validation shall be in the form of a letter scheduling the validation and the subsequent delivery by the offeror of a CSL registered report or CSL certificate immediately upon receipt thereof. Proof of testing shall be provided in the form of a CSL registered validation summary report. Proof of validation shall be in the form of a CSL Certificate of Validation.

"Prior Validation Testing"

> The offeror shall certify in the offer that all implementations of FIPS, including applicable FIPS options, offered in response to this document have been previously tested or validated and included on the current list of validated products maintained by the Computer Systems Laboratory (CSL). Unless specified elsewhere, proof of testing shall be provided in the form of a CSL registered validation summary report. Proof of validation shall be in the form of a CSL Certificate of Validation.

"Prior Validation"

> The offeror shall certify in the offer that all implementation of FIPS,

including applicable FIPS options, offered in response to this document have been previously validated and included on the current list of validated products maintained by Computer Systems Laboratory (CSL). Unless specified elsewhere, proof of validation shall be in the form of a CSL Certificate of Validation.

Appendix C

Planning Phase Risk Analysis

A planning phase risk analysis is similar to a "regular" risk analysis. They share the same goal and overall strategy. The goal is to identify vulnerabilities and offsetting controls. The logical outcome of any risk analysis is the acquisition and/or implementation of cost-effective security controls. This is often referred to as the risk reduction phase. (Another product of the risk analysis is the identification of residual risk which cannot be further reduced or eliminated in an economically feasible manner by currently available means.)

The strategy of a risk analysis is to examine potential losses that may result from weaknesses in system security and the damage that may result from the occurrence of certain threats. In order to do this, a risk analysis contains the following components:

- Asset identification and valuation
- Threat analysis
- Vulnerability assessment
- Impact analysis
- Determination of risk

Since the goal of a risk analysis is the selection of cost-effective safeguards, a risk analysis is actually a decision-support tool. By identifying those areas with the greatest potential for loss or harm, the risk analysis provides a basis for a system manager to make informed choices about controls. This allows the manager to allocate precious resources based on need and expected effectiveness.

The planning phase risk analysis is performed during the planning stage of system acquisition and during the design stage of a system life cycle. As discussed in section III.B.1.b and section III.B.2, this analysis is used as a basis for deciding which safeguards are mandatory and which are desirable. The analysis should, therefore, concentrate on items that are related to system acquisition decisions. In addition, it will help support the evaluation plan's ranking of the desirable safeguards.

As the term "planning phase" implies, further risk analysis is required during the life of a system. OMB Circular A-130 requires periodic risk analysis for general support systems. However, depending on the nature of the system, how it is being developed or acquired, and other factors, there are many places during the systems life when a form of risk analysis may be useful. In general, risk analysis should be viewed as an iterative process to take into account changes in the system, the system environment, and knowledge about the system. The nature of the risk analysis should always be commensurate with the placement in the systems life and the sensitivity of the system.

How to Perform a Planning Phase Risk Analysis

Although a planning phase risk analysis is very much like a risk analysis, there are differences. A planning phase risk analysis is less precise. The analysis considers projected costs, assets, threats and vulnerabilities, not current ones. The impacts of failures are based on a projection of system

use. The emphasis of risk analysis is the assessment of existing assets and controls. The planning phase risk analysis emphasizes the impacts of possible security problems and how to mitigate them.

The planning phase risk analysis should be performed in keeping with federal and agency guidance. The agency risk analysis office or computer security office should be consulted.

The planning phase risk analysis need not be a large and complex document. It should focus on defining and documenting system security requirements. The purpose of a risk analysis is not to spend a lot of time trying to quantify or describe assets and impacts but to provide a basis for making informed decisions about system security. Therefore, the level of detail should be commensurate with the sensitivity of the system and the need for decision support.

Existing agency risk analyses can be used as a starting point. Since many information processing resources are bought as part of either an existing facility, application, or system, many aspects including physical, application, user, and facility environment may already be known.

A planning phase risk analysis methodology based on the FIRMR, Federal Information Processing Standard Publication (FIPS PUB) 73 and other source material is presented in GAO Report Agencies Overlook Security Controls During Development (GAO/IMTEC-88-11S) and reprinted below. Additional material on risk analysis is available from the sources referenced in the GAO report and from:

Special Publication 500-174	Guide for Selecting Automated Risk Analysis Tools
NISTIR 4325	U.S. Department of Energy Risk Assessment Methodology
NISTIR 4749	Sample Statements of Work for Federal Computer Security Services.

GAO Methodology

This is a risk methodology, based on a system development life cycle, published by the GAO. Agencies can use other methodologies or modify this one. Nothing in this methodology is required. The methodology does not provide much detail; the references cited above and in the methodology can be used to provide additional guidance. (Note: FIRMR citations are from the 1988 version.)

Initial Risks

1. Identify the impact of major failure including:
   a. an analysis of expected losses calculated in dollars or other significant indicators (FIRMR, Section 201-7.103-2) such as (FIPS 73, p. 27):
      1. extent of inconvenience or hardship to individuals.
      2. extent of lives lost.
      3. extent of disruption to the national economy or national security.
   b. an analysis of, but is not limited to, the impact of the following risks (FIRMR, Section 201-7.103-2):

1. physical destruction or loss of data and program files (also in FIPS 73, p. 27; FIPS 31, p. 10).
2. theft or disclosure of information (also in FIPS 73, p. 7), data confidentiality issues (FIPS 65, p. 9), improper dissemination and careless disposal (FIPS 41, p. 12)
3. misuse of ADP system, that is, fraud, vandalism, etc., (see also falsified data, FIPS 73, p. 27; theft of information or assets, FIPS 31, p. 10).
4. delay or prevention of ADP operation (see also unavailable data or services, FIPS 73, p. 27).
5. lack of reliability of automated data processing equipment and utilities.
6. altered or inaccurate data (also in FIPS 73, p. 25).

c. potential impacts are assessed for every application that will maintain or process sensitive or mission-critical information (implied in FIPS 73, p. 27).

2. Estimate the frequency of major failure in the areas of:
   a. inaccurate data,
   b. falsified data,
   c. disclosed data,
   d. lost data or programs, and
   e. unavailable data or services (FIPS 73, p. 27).

3. Estimate the cost of major failures:
   a. Calculate an annual loss expectancy that combines the estimates of the value of potential loss and probability of loss (FIPS 31, p. 11). See prior risk section (2C.1.,2) for the impact and frequency of failure estimates that the agency should include in its analysis.
   b. Remedial security measures are identified to address significant threats (FIPS 31, p. 13) and vulnerabilities (FIPS 73, p. 25), including measures such as:
      1. altering the environment (FIPS 31, p. 13),
      2. erecting barriers (FIPS 31, p. 13),
      3. improving procedures (FIPS 31, p. 13),
      4. early detection (FIPS 31, p. 13), and
      5. contingency plans (FIPS 31, p. 13).
   c. The cost of remedial measures is identified including an identification of the least cost mix of security measures (FIPS 31, p. 13).

GLOSSARY

Acceptance The act of an authorized representative of the government by which the government, for itself or as agent of another, assumes control or ownership of existing identified supplies tendered or approves specific services rendered as partial or complete performance of the contract. It is the final determination whether or not a facility or system meets the specified technical and performance standards.

Access control Specifically computer systems access control. Restrictions on the types of interactions between subjects (i.e., persons) and objects (i.e., files or data elements). Access can be divided into types of access such as read, write, modify, or execute. (Access control also includes physical access control.)

Acquisition Acquiring by contract with appropriated funds supplies or services by and for the use of the federal government through purchase or lease, whether the supplies or services are already in existence, or must be created, developed, demonstrated, and evaluated. Acquisition begins at the point when agency needs are established and includes the description of requirements to satisfy agency needs, solicitation and selection of sources, award of contract, contract financing, contract performance, contract administration and those technical and management function directly related to the process of fulfilling agency needs by contract. See also procurement.

Accreditation A critical management decision made by an agency official regarding the adequacy of security safeguards, i.e., whether the safeguards reduce risk to an acceptable level for the intended function. It must be based on reliable technical information. It is the approval to operate a computer system. See certification.

ADP Automatic data processing. ADP refers to the resources used to process automated information, including telecommunications. The FIRMR now uses the term Federal Information Processing (FIP) resources.

Administration Specifically contract administration. Government management of a contract to ensure that the government receives the quality of products and services specified in the contract within established costs and schedules.

Analysis of integrity, availability, and confidentiality requirements An analysis of the protection requirements of a system based on the system's need for integrity, availability, and/or confidentiality.

Analysis of level of assurance An analysis of the level of confidence needed that the security of a system will work correctly and will be effective. This analysis forms the basis for the procurement evaluation plan and/or acceptance plan.

Assurance A measure of confidence that the security features and architecture of a computer system meet the security requirements.

Authenticate To establish the validity of a claimed identity.

BAFO Best and Final Offer. An opportunity for offerors in the competitive

range to submit final proposals.

Bidder Any entity that responds to an invitation for bids with a bid. See offeror.

Benchmark A test of the capabilities of a proposed system using customized workloads

Certification
1) Security certification A technical analysis of a system or application relative to a set of system requirements used for the purpose of accreditation. See accreditation.
2) Security certification A technical analysis and formal declaration by an agency official that an application or system meets all applicable federal policies, regulations, and standards, and that safeguards are adequate for the application.
3) Procurement certification A signed statement by an offeror.

Closeout Includes all final contract activities, e.g., ensuring completion of all requirements, making the final payment.

Commercial off-the-shelf (COTS) Software and hardware that already exists. It is also referred to as off-the-shelf.

Competition in Contracting Act of 1984 (CICA) A statute that made several revisions to federal contracting including requiring that specifications be developed in an "unrestricted manner" to obtain full and open competition.

Computer Security The protection of automatic data processing assets from harm. This includes the protection of data, hardware, firmware, and software. Harm is defined as a loss of integrity, availability, or confidentiality.

Computer Security Act of 1987 A statute "to provide for a computer standards program with the (National Institute of Standards and Technology), to provide for government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of federal computer systems, and for other purposes."

Confidential Private, nondisclosable. (In this guideline confidential never refers to classified material.)

Contingency planning Plans to assure that users can continue to perform essential functions and that a reasonable continuity of data processing support is provided at all times. These plans can include emergency response, backup operation, and post-disaster recovery.

Contracting Officer (CO) A person with the authority to enter into, administer, and/or terminate contracts and make related determination and findings.

Contracting Officer's Technical Representative (COTR) An individual to whom the Contracting Officer delegates certain contract responsibilities, usually related to technical direction and acceptance issues. Also called Government Technical Representative (GTR) or the Contracting Officer's Representative (COR).

DAC See discretionary access control.

Delegation of Procurement Authority (DPA) A grant of authority by GSA to acquire FIP resources or services. See section II.B.2.

Deliverable A product or service that is prepared for and delivered to the government under the terms of a contract.

DES Data Encryption Standard. FIPS PUB 46-1. Specifies an algorithm to be implemented for cryptographic protection of sensitive data.

Discretionary access control A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject. See access control and mandatory access control.

Directed specification A specification that must be included in statements of work based on federal law, policy, or regulation.

Domain The unique context in which a program is operating.

Evaluation
1) Security evaluation The examination of the technical and nontechnical security features of a computer system and other safeguards that establishes the extent to which a particular design and implementation meet a specified set of security requirements.
2) Procurement technical evaluation The examination of proposals in order to determine technical acceptability and merit. This is part of the source selection process.
3) Product security evaluation The examination of the security features of a product against a stated set of requirements or criteria. Product evaluations are often performed in a laboratory setting.

Federal Acquisition Regulation (FAR) The regulation that codifies uniform acquisition policies and procedures for Executive agencies.

Federal Information Processing (FIP) FIP refers to the resources and services used to process automated information, including telecommunications.

Federal Information Resources Management Regulation (FIRMR) The regulation that sets forth uniform policies and procedures pertaining to acquisition of information resources; used in conjunction with the FAR.

Features Specifically technical security features. The security-relevant functions, mechanisms, and characteristics of system hardware, firmware, and software. Technical security features are a subset of system security safeguards.

FIPS PUB Federal Information Processing Standards Publication

Flowdown The extension of prime contractor requirements to subcontractors.

Full and open competition The consideration of all responsible sources in a procurement, as required by the Competition in Contracting Act.

GSBCA General Services Board of Contract Appeals.

GTR Government Technical Representative. See Contracting Officer's Technical Representative.

IFB Invitation for Bid. A solicitation document used when contracting by sealed bids.

ITSEC Information Technology Security Evaluation Criteria. The harmonized security criteria of France, Germany, the Netherlands and the United Kingdom.

IV&V Independent Verification and Validation.

Label
1) Security label A piece of information that tells a system how to handle data. The label can be used to control access, specify protective measures, or indicate handling restrictions required by a security policy.
2) Access control label A piece of information that represents the security level or sensitivity designation of data in an object or the access authorization of a subject.

Latent defects Defects that exist at the time of acceptance but are not discoverable by a reasonable inspection.

Liquidated damages Compensation to the government for damages that result from the contractor failing to deliver supplies or perform services. (See FAR 12.2 and 52.212-4).

Live test demonstrations (LTDs) The demonstration of capability or period of time during which a government user requires an offeror to perform certain user-witnessed activities. These can include one or more benchmark tests. These occur prior to contract award.

MAC Message authentication code or mandatory access control.

Mandatory access control A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization of subjects to access information of such sensitivity. In a mandatory access control environment, users cannot pass their access rights to others without express concurrence of the access control authority. See access control and discretionary access control.

Mandatory requirements Those contractual conditions and technical specifications that are established by the government as being essential to meeting required needs.

Mechanism Specifically security mechanism. See safeguard.

Multi-label Having information with different sensitivities on one system. A multi-label secure system permits simultaneous access by users not authorized by the mandatory access authority to access all of the data and prevents unauthorized access. This term is normally used to describe systems with nonhierarchical information sensitivities and where the system is relied upon to enforce a mandatory policy. See label and multilevel.

Multilevel Having information with different sensitivities on one system. A multilevel secure system permits simultaneous access by users not authorized by the mandatory access authority to access all of the data and prevents unauthorized access. This term is normally used to describe systems with

hierarchical information sensitivities and where the system is relied upon to enforce a mandatory policy. See multi-label.

Needs determination An assessment, performed as part of initial system planning, which looks at the needs of an agency that might be met through automation.

Object A passive entity that contains or receives information. Access to an object implies access to the information it contains. Examples of objects are: records, blocks, files, programs, video displays, printers, network nodes, etc.

Object reuse The removal of residual data from a system resource prior to reassignment and reuse.

Off-the-shelf Software and hardware that already exists. It is also referred to as commercial off-the-shelf (COTS).

Offeror Any entity that responds to an RFP with a proposal. See bidder.

Orange Book See TCSEC.

Preaward survey An evaluation by a surveying activity of a prospective contractor's capability to perform a proposed contract.

Presolicitation The period preceding release of a solicitation that includes preparation of documentation required by federal regulations.

Procedure Specifically security procedure. A type of safeguard based on human actions (as opposed to technical features). These can be referred to as administrative safeguards.

Procurement Includes all stages of the process of acquiring property or services, beginning with the process for determining need for the property or services and ending with contract completion and closeout.

Procurement initiator The key person who represents the program office in formulating information resources requirements and managing presolicitation activities. Also called program manager, sponsor. This person often becomes the contracting officer's technical representative (COTR).

Program manager See procurement initiator.

Protest A written objection by an interested party to a solicitation for a proposed contract for the acquisition of supplies or services or a written objection by an interested party to a proposed award or the award of such a contract.

RFC Request for Comment. An announcement requesting industry comment on a proposed system or other acquisition.

RFI Request for Information. An announcement requesting information from industry in regard to a planned acquisition and, in some cases, requesting corporate capability information.

RFP Request for Proposals. A solicitation document used in negotiated acquisitions to communicate government requirements and to solicit proposals.

RFQ Request for Quotation. A solicitation document used in negotiated acquisitions to communicate government requirements and to solicit quotations.

Requirements analysis A part of the acquisition cycle in which the requirements for a system are developed.

Responsible prospective contractor To be responsible, a prospective contractor must meet the requirements of FAR 9.104-1 which include the ability to be able perform the contract based on the financial, technical, organizational, ethical, and legal position of the contractor.

Responsive prospective contractor To be responsive, a prospective contractor must comply in all material respects with the solicitation.

Restrictive specification A detailed and precise description of an item(s) being acquired that needlessly limits competition, e.g., "brand name" without the words "or equal."

Risk analysis The process of examining assets, threats, and vulnerabilities in order to determine cost-effective security controls.

Safeguard Any action, device, feature, mechanism, procedure, technique, or other measure that reduces the vulnerability of or threat to a system. Also called controls or countermeasures.

Sensitive information Any information which the loss, misuse, modification of, or unauthorized access to, could affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but that has not been specifically authorized under criteria established by an Executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.

Sensitivity assessment An initial assessment of the general sensitivity of an agency function.

Single-label A subset of a multi-label system in which only one type of labeled information is processed at a time. See label and multi-label.

Solicitation An official government request for bids/proposals often publicized in the Commerce Business Daily.

Source selection The process of evaluating proposals and determining which offeror will be selected for contract award.

SEB Source Evaluation Board. A board comprised of technical, contract, information resources management, and other representatives whose primary function is to evaluate proposals received in response to an RFP.

Specification A description of the technical requirements for a material, product, or service. Specifications should state only the government's actual minimum needs and be designed to promote full and open competition, with due regard for the nature of the services to be acquired.

Sponsor See procurement initiator.

Statement of work (SOW) A statement of the technical specification in the RFP that describes the work or system required by the government.

Subject An active entity, generally a person, process, or device that causes actions such as the flow of information.

TCSEC Trusted Computer System Evaluation Criteria. DoD 5200.28-STD. The Department of Defense security evaluation criteria. Also called the Orange Book.

Threat Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.

Trusted computing base (TCB) Specifically DoD 5200.28. The totality of protection mechanisms within a computer system -- including hardware, firmware, and software -- that are responsible for enforcing a security policy.

Vetting Specifically personnel vetting. The process of investigating personnel with the intent to approve or disapprove access to government resources. The investigations can range from minimal checks to full background investigations. Also called personnel screening.

Vulnerability A weakness in system security procedures, system design, implementation, internal controls, physical environment, etc.

Warner Amendment 10 USCA 2315. Excludes certain systems from the requirements of Section 111 of the Federal Property and Administrative Services Act of 1949 (40 USC 795), including automatic data processing equipment or services if the function, operation, or use of the equipment of services involves intelligence activities, involves cryptographic activities related to national security, involves the command and control of military forces, equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions except for equipment or services to be used for routine administrative and business application (including payroll, finance, logistics, and personnel management applications).

Appendix E

References

Acquisition of Information Resources: Overview Guide, U.S. General Services Administration; January 1990.

Boehm, B. W., "Software Engineering." IEEE Transactions on Computers, C-25, December, 1976.

Agencies Overlook Security Controls During Development, General Accounting Office Report to the Chairman, Committee on Science, Spec, and technology, House of Representative; May 1988; GAO/IMTEC-88-11 and GAO/IMTEC-88-11S.

Computer Security Act of 1987, Public Law 100-235.

Department of Defense Trusted Computer System Evaluation Criteria, Department of Defense; December 1985; DOD 5200.28-STD.

Federal Acquisition Regulation, Department of Defense, General Services Administration and National Aeronautics and Space Administration.

Federal ADP & Telecommunications Standards Index, General Services Administration; April, 1991.

Federal Information Resources Management Regulation, General Services Administration; 41 CFR 201.

Federal Personnel Manual, Chapters 731, 732, and 736, Office of Personnel Management.

Frankel, S. ed. Guidance on Software Package Selection, National Bureau of Standards (U.S.); November 1986; Special Publication 500-144.

Gilbert, Dennis, et al, Sample Statements of Work for Federal Computer Security Services, National Institute of Standards and Technology; November 1991; NIST Interagency Report 4749.

Gilbert, Irene, Guide for Selecting Automated Risk Analysis Tools, National Institute of Standards and Technology; October 1989; Special Publication 500-174.

Glossary of Computer Security Terms, National Computer Security Center; October 1988; NCSC-TG-004.

Guidance to Federal Agencies on the Use of Trusted Systems Technology, National Institute of Standards and Technology; July 1990; NCSL Bulletin.

Guideline for Computer Security Certification and Accreditation, National Bureau of Standards (U.S.); September 1983; FIPS PUB 102.

Guidelines for Security of Computer Applications, National Bureau of Standards (U.S.); June 1980; FIPS PUB 73.

Information Technology Security Evaluation Criteria, Herausgeber: Der Bundesminister des Inner, Bonn, Mai 1990.

Kiely, John, Assuring the Integrity of Purchased Software, Computer Security Institute 17th Annual Computer Security Conference; November 1990.

Model Framework for Management Control Over Automated Information Systems, President's Council on Management Improvement and the President's Council on Integrity and Efficiency; January 1988.

NASA Automated Information Security Handbook, National Aeronautics and Space Administration; September 1990; NASA Handbook 2410.9.

Office of Management and Budget Circular A-130, Management of Federal Information Resources, December 1985.

Review of General Controls in Federal Computer Systems, President's Council on Integrity and Efficiency; October 1988.

Ruthberg, Zella G et al, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach, National Bureau of Standards (U.S.); April 1988; Special Publication 500-153.

Standard Security Label for the Government Open Systems Interconnection Profile, National Institute of Standards and Technology; February 28, 1991; draft FIPS PUB.

Todd, Mary Ann and Constance Guitian, Computer Security Training Guidelines, National Institute of Standards and Technology; November 1989; Special Publication 500-172.

U.S. Department of Energy Risk Assessment Methodology, National Institute of Standards and Technology; May, 1990, Interagency Report 4325.

Wallace, Dolores R. and John C. Cherniavsky, Guide to Software Acceptance, National Institute of Standards and Technology, April 1990; Special Publication 500-180.

Wallace, Dolores and Roger Fujii, Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Product Management Standards, National Institute of Standards and Technology; September 1989, Special Publication 500-165.